January
2005
Volume 53
Number 1

United States
Department of Justice
Executive Office for
United States Attorneys
Office of Legal Education
Washington, DC
20535

Mary Beth Buchanan
Director

Contributors' opinions and statements should not be considered an endorsement by EOUSA for any policy, program, or service.

The United States Attorneys' Bulletin is published pursuant to 28 CFR § 0.22(b).

The United States Attorneys' Bulletin is published bi-monthly by the Executive Office for United States Attorneys, Office of Legal Education, 1620 Pendleton Street, Columbia, South Carolina 29201. Periodical postage paid at Washington, D.C. Postmaster: Send address changes to Editor, United States Attorneys' Bulletin, Office of Legal Education, 1620 Pendleton Street, Columbia, South Carolina 29201.

Managing Editor
Jim Donovan

Technical Editor
Nancy Bowman

Law Clerk
Carolyn Perozzi

Internet Address
www.usdoj.gov/usao/reading_room/foiamanuals.html

Send article submissions to Managing Editor, United States Attorneys' Bulletin, National Advocacy Center, Office of Legal Education, 1620 Pendleton Street, Columbia, SC 29201.

Social Security Fraud

In This Issue

Prosecuting Social Security Number Misuse: Attacking Identity Theft at its Source

John K. Webb
Special Assistant United States Attorney
Central District of California

"Good name in man and woman . . . is the immediate jewel of their souls. Who steals my purse steals trash . . . but he that filches from me my good name robs me of that which not enriches him and makes me poor indeed."

WILLIAM SHAKESPEARE, OTHELLO, act 3, sc. 3.

I. Introduction

Protection of the Social Security Number (SSN) is inherent to maintaining personal privacy and in assuring that no one "filches" your good name. In fact, failure to carefully guard the SSN could make one "poor indeed." As any victim of identity theft will tell you, not much has changed since the days of Shakespeare when it comes to "filching," and thieves continue to roam the streets looking for victims to rob of their good name. Indeed, today's robbers have incorporated the use of cyberspace into their bag of dirty tricks, and the theft and misuse of the SSN is the most common tool that identity thieves employ. The misuse of the SSN poses a risk to public safety and a threat to the personal privacy and financial security of every American.

The SSN has been with us since 1936 and was first intended for use solely by the federal government as a means of tracking earnings to determine the amount of Social Security taxes to credit to each worker's account. Use of the SSN for purposes unrelated to the administration of the Social Security system is a relatively recent phenomenon. Over the years, the SSN has been used by government agencies and the private sector for other purposes, often over the objection of independent experts and the general public. *See*, *e.g.*, ALAN WESTIN & MICHAEL BAKER, DATABANKS IN A FREE SOCIETY, 399 (Times Books 1972) ("adopting the Social Security number officially as a national identifier or letting its use spread unchecked cannot help but contribute to public distrust of government").

A. SSN misuse, identity theft, and the risk to personal and financial privacy

Today, the SSN is a fundamental element of almost every identity theft case, and Congress has long recognized that disclosure of the SSN is a threat to individual privacy. *See* Privacy Act, Pub. L. No. 93-579, 88 Stat. 1896 (1974). With the enactment of the Privacy Act in 1974, Congress explicitly recognized the particular risk to privacy brought about by the threat of the misuse and unnecessary disclosure of the SSN and enacted express restrictions on the use of the SSN. *Id*. The extent of the threat to individual privacy is readily apparent when considering that the SSN is used as an identification code that brings individuals into contact for everyday communication with databases containing a wide range of financial, medical, educational, and credit information. Once obtained by an identity thief, the SSN opens practically every door related to a person's identity and personal history and completely compromises an individual's personal privacy. The development and expansion of the Internet has contributed significantly to the danger of identity theft that is inherent to disclosure of the SSN. As the Supreme Court noted, the Privacy Act "was passed in 1974 largely out of concern over 'the impact of computer data banks on individual privacy.'" *See United States Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749, 765 (1989). Today, even with the explosion of identity theft, the demand continues for disclosure of an individual's SSN for purposes unrelated to its intended use. The result is the frequent and indiscriminate use and disclosure of the SSN as part of identity theft crimes.

B. History of the SSN and restrictions on its use

On August 14, 1935, Congress enacted legislation creating the Social Security Administration (SSA). *See* Social Security Act (the Social Security Act of 1935), Pub. L. No. 74-271, 49 Stat. 620 (1935). The purpose of the Social Security Act (the Act) was the creation and implementation of a social insurance program designed to pay benefits to retired workers to ensure a continuing portion of income after retirement. *Id*. The amount of these social benefits was based, in part, on the amount of the workers' earnings, and SSA needed a system to keep track of earnings by individual workers and for employers to report these earnings. Included in the Act was authorization for SSA to establish a record-keeping system to help manage the Social Security program. While it did not expressly mention the use of the SSN, the Act authorized the creation of some type of record keeping scheme. Thus, on or about November 24, 1936, the first applications for Social Security account numbers (Form SS-5) were distributed by the Post Office to persons who were working or expected to work in jobs covered by Social Security old-age insurance. *See* "Special Collections-Chronology" (Social Security Online), *available at* http://www.ssa.gov/history/1930.html. Through a process known as enumeration, unique numbers were created by SSA for every person, and used by SSA and the Internal Revenue Service (IRS) as a work and retirement benefit record for the Social Security program. *Id*. In accordance with the establishment of the SSN as a record keeping tool, the IRS issued a regulation in 1936 that required the issuance of an account number to each employee covered by the Social Security program. *See* Treasury Decision 4704 (1936). Between November 1936 and June 1937, SSA processed approximately thirty million SS-5 Forms. *Available at* http://www.ssa.gov/history/ssn/firstcard.html.

The process of issuing Social Security Numbers continues today, with SSA issuing them to all U.S. citizens and most noncitizens who are lawfully admitted to the United States and who have permission to work. *Available at* http://www.ssa.gov/ssnumber. Lawfully admitted noncitizens may also qualify for an SSN for nonwork purposes when a federal, state, or local law requires that an SSN be obtained in order to receive a particular welfare benefit or service. SSA collects and verifies information from such applicants regarding their age, identity, citizenship, and immigration status. Most of SSA's enumeration workload involves U.S. citizens who generally receive an SSN via SSA's birth registration process handled by hospitals. However, individuals seeking SSN's can also apply in person at any SSA field office location, through the mail, or via the Internet. *See* http://www.ssa.gov/ssnumber. Most U.S. born individuals receive an SSN through a process SSA refers to as Enumeration-at-Birth (EAB). Under EAB parents can apply for an SSN for their newborn child at the hospital as part of the birth registration process. Under this process, hospitals send birth registration information to a state or local bureau of vital statistics where it is entered into a database. The appropriate bureau of vital statistics forwards SSA the required information, usually by electronic means. SSA accepts the data captured during the birth registration process as evidence of age, identity, and citizenship, and assigns the child an SSN without further parental involvement. Once SSA receives the required information, it performs edits, assigns the SSN, and issues the card. *See Social Security Numbers: Insuring the Integrity of the SSN* GAO REP. 03-941T (2003), *available at* http://www.gao.gov/new.items/d03941t.pdf.

Widespread SSN use in government began with a 1943 Executive Order issued by President Franklin D. Roosevelt. *See* Exec. Order No. 9,397, 3 C.F.R. 283-284 (1943-1948). Specifically, the order required all federal components to use the SSN exclusively whenever the component needed to set up a new identification system for individuals, and instructed the Social Security Board to cooperate with federal uses of the SSN by issuing and verifying numbers for other federal agencies. *Id*. Since 1943, the number of federal agencies and others relying on the SSN as a primary identifier has escalated dramatically, in part, because a number of federal laws have been passed that have authorized or required use of the SSN for specific activities. *See Social Security Numbers: Government Benefits from SSN Use but Could Provide Better Safeguards* GAO REP. 02-352 (2002), *available at* http://www.gao.gov/new.items/d02352.pdf. In many instances, use of an SSN is required by law to determine the eligibility of an individual for receipt of federally funded program services or benefits, such as SSA Title II benefits (Retirement, Disability, or Survivor's) or

Supplemental Security Income (SSI) benefits payments. Use of the SSN also serves as a unique identifier for such government-related activities as paying taxes or reporting wages and earnings. The government was first permitted to use the SSN for tax reporting purposes in 1961, when Congress authorized the IRS to use the SSN as taxpayer identification numbers. *See* Pub. L. No. 87-397, 75 Stat. 828 (1961).

Since issuance of the first SSN in 1936, the private sector, for all practical purposes, has taken control of the SSN. Individuals must now provide it when applying for credit, when seeking medical or other insurance coverage, for leasing an apartment, seeking cell phone service, ordering merchandise, or applying for a job. In addition, many federal, state, and local government agencies also use the SSN as a means of identification when they administer their programs to deliver services or benefits to the public. In some instances, government agencies serve as the repository for records or documents that are routinely made available to the public for inspection. These public records may include SSNs. *See Social Security: Government and Commercial Use of the Social Security Number is Widespread* GAO REP. 99-28 (1999), *available at* http://www.gao.gov/archive/1999/he99028.pdf. This growth in use and availability of the SSN is important because SSNs are often the identifier of choice among identity thieves. No single federal law regulates overall use and disclosure of SSNs by federal agencies, but several federal laws limit the use and disclosure of the SSN in certain circumstances. *See* 42 U.S.C. § 408(a)(7)(B); *see also* 18 U.S.C. § 1028(a)(7) and 18 U.S.C. § 1028A. State laws may also vary in terms of the restrictions imposed on SSN use and disclosure. Moreover, some records that contain SSNs are considered part of the public record and, as such, are routinely made available to the public for review. *See Social Security Numbers: Government Benefits from SSN Use, but Could Provide Better Safeguards* GAO REP. 02-352 (2002), *available at* http://www.gao.gov/new.items/d02352.pdf.

It goes without saying that the SSN is a key piece of identification in building credit bureau databases, extracting or retrieving data from consumers' credit histories, and preventing fraud. *See* Prepared statement of the FTC, *Identity Theft: the FTC's Response: Hearing Before the Subcommittee on Technology, Terrorism and Government Information, Senate Judiciary Committee*, 107th Cong. (Mar. 20, 2002), *available at* http://www.consumer.gov/idtheft_old/reports.htm. Businesses routinely report consumers' financial transactions, such as charges, loans, and credit repayments to credit bureaus. Although credit bureaus use other identifiers, such as names and addresses, to build and maintain individuals' credit histories, the SSN is the most important identifier for ensuring that correct information is associated with the right individual, because the SSN does not change as would a name or address. The SSN, along with names and birth certificates, are three personal identifiers most often sought by identity thieves. *See Identity Theft: Prevalence and Cost Appear to be Growing* GAO REP. 02-363 (2002), *available at* http://www.consumer.gov/idtheft/reports/gao-d02363.pdf.

Identity theft occurs when an individual steals another individual's personal identifying information and uses it fraudulently. It is a crime that can affect all Americans. SSNs and other personal information, for example, are used to fraudulently obtain credit cards, open utility accounts, access existing financial accounts, commit bank fraud, file false tax returns, and falsely obtain employment and government benefits. The SSN plays an important role in identity theft because it is used as breeder information to create additional false identification documents, such as drivers' licenses, Social Security cards, I-9 and W-4 forms, and green cards. Most often, identity thieves use SSNs belonging to real people, rather than making one up. However, identity thieves sometimes merely make up a number that happens to correspond to an SSN already assigned to an individual by the Commissioner of Social Security. Most often, identity thieves gain access to the personal information of a victim by:

- taking advantage of an existing relationship with the victim;
- stealing information from purses, wallets, or the mail;
- purchasing personal information from a coworker of the victim; and
- identifying personal information obtained legally through Internet sites maintained by both the public and private sectors (including data from records routinely made available to the public through the court system).

See Identity Theft: Prevalence and Cost Appear to be Growing GAO REP. 02-363 (2002), *available at* http://www.consumer.gov/idtheft/reports/gao-d02363.pdf.

II. Legislative history regarding disclosure and criminal misuse of the SSN

In recent years Congress has become increasingly sensitive to the problem of identity theft, and Congressional committees have conducted frequent hearings in preparation for offering various legislative solutions to combat the danger. Debate regarding legislation opposing disclosure of the SSN is a common issue discussed during these committee hearings. The recent attention to the SSN, however, is nothing new, for Congress has been aware of public opposition to the misuse of the SSN since the 1970s, when a series of hearings were held on privacy and information collection. *See*, e.g., *Federal Data Banks, Computers and the Bill of Rights: Hearings Before the Subcommittee on Constitutional Rights of the Senate Judiciary Committee*, 92d Cong.775-881 (1971) (statement of Elliot Richardson, Secretary of Health, Education and Welfare (HEW)). In this hearing, Secretary Richardson testified that:

> [t]here would certainly be an enormous convenience in having a single identifier for each individual...[making] more efficient the acquisition, storage, and use of data.... It is the very ease of assembling complete records, of course, which raises the specter of invasion of privacy.

Id. at 784.

A. The 1973 HEW Report on Safeguards for Federal Records Systems

In 1973 an advisory committee to the HEW issued a report that recommended the development of extensive legal safeguards for record systems maintained by the federal government. *See Secretary's Advisory Committee on Automated Personal Data Systems: Records, Computers and the Rights of Citizens* (HEW Report) HEW, 121 (1973), *available at* http://aspe.hhs.gov/datacncl/1973privacy/tocprefacemembers.htm. The advisory committee warned that the use of the SSN as a personal identifier "would enhance the likelihood of arbitrary or uncontrolled linkage of records about people, particularly between government or government-supported automated personal data systems...." *Id.* at 122. Based on their findings, the advisory committee recommended the enactment of restrictions on the disclosure and dissemination of the SSN, including:

- Uses of the Social Security Number should be limited to only those purposes required by the federal government.
- Federal agencies should not require the use of the Social Security Number absent statutory authority.
- Congress should evaluate any proposed use of the Social Security Number.
- Individuals have the right to refuse to provide their Social Security Numbers and should suffer no harm for exercising this right.
- Organizations required by federal law to obtain the Social Security Number should use the number solely for the purpose for which it was obtained and not make any secondary use or disclose the SSN without the informed consent of the individual.

Id. at 124-25.

B. Enactment of the 1974 Privacy Act

In response to the 1973 HEW Report Congress adopted recommendations made by the advisory committee through passage of the 1974 Privacy Act. *See* Pub. Law No. 93-579, 88 Stat. 1896 (1974); *see also* S. REP. NO. 1183 (1974), *reprinted in* 1974 U.S.C.C.A.N. 6916, 6944-46 (citing HEW Report). A reading of the Privacy Act clearly shows that Congress gave special attention to the need to control the proliferation and misuse of the SSN. For example, § 7 of the Privacy Act makes it unlawful for any agency to deny any right, benefit, or privilege, to any individual "because of such individual's refusal to disclose his social security account number." The Act further provides that any agency requesting an individual to disclose his SSN must "inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it." *See* Pub. L. No. 93-579, § 7, 88 Stat. 1896, 1909 (1974), *reprinted in* 5 U.S.C. § 552 (1982). By enacting these protections, Congress

sought to prevent the privacy violations made possible by the proliferation of the SSN.

C. Criminalizing disclosure and misuse of the SSN under the Social Security Act

Consistent with the concerns it expressed in the enactment of the Privacy Act, Congress moved to penalize the disclosure and misuse of the SSN by a series of amendments to the Social Security Act. Beginning in 1972, Congress amended the Act to add misdemeanor penalties for fraudulent use of the SSN. In response to growing concerns about individual privacy and the damage that could occur from the fraudulent misuse of a person's identity and SSN, the Act was amended again in 1974 and 1981 to make SSN misuse a felony.

In 1972 misdemeanor fraud provisions were first added to the Act. These provisions were designed by Congress for the sole purpose of preventing any person from obtaining federal benefits by using a fraudulent SSN. Specifically, the Act's 1972 fraud subsection forbade anyone from using a Social Security Number to increase any payment or to obtain any improper payment or benefit under any federal program. *See* Social Security Amendments of 1972, Pub. L. No. 92-603, § 130(a), *reprinted in* 1972 U.S.C.C.A.N. 1548, 1586; *see also* H.R. CONF. REP. NO. 92-1605 (1972), *reprinted in* 1972 U.S.C.C.A.N. 4989, 5370, 5373 (citing prevention of improper benefit payments as the sole purpose behind the new provisions).

In 1976 the reach of the SSA fraud penalty was expanded substantially when the Act was amended to include not only those who sought unauthorized or excessive federal benefits, but also those who misused Social Security Numbers "for any other purpose." (*See* Tax Reform Act of 1976, Pub. L. No. 94-455, § 1211, 90 Stat. 1520, 1711 (1976); *codified at* 42 U.S.C. § 405(c)(2)(C)(i) (the 1976 Act). The House Conference Report to the 1976 Act spoke directly to the broadened statutory language, stating:

> [The Senate amendment] makes a misdemeanor the willful, knowing, and deceitful use of a social security number for any purpose. In addition, the Senate amendment changes the Privacy Act so that a State or political subdivision may use social security numbers for the purpose of establishing the identification of individuals affected by any tax, general public assistance, driver's license, and motor vehicle registration laws.

See H.R. CONF. REP. NO. 94-1515 (1976), *reprinted in* 1976 U.S.C.C.A.N. 2897, 4030, 4118, 4194-95.

In a particularly revealing and crucial portion of the legislative history of the 1976 amendments, the 1976 report of the Senate Finance Committee also sought to explain the addition of the words "for any other purpose" to the Act:

> While the Social Security Act currently provides criminal penalties for the wrongful use of a social security number for the purpose of obtaining or increasing certain benefit payments, including social security benefits, there is no provision in the Code or in the Social Security Act relating to the use of a social security number for purposes unrelated to benefit payments. The committee believes that social security numbers should not be wrongfully used for any purpose.

See S. REP. NO. 94-938(I) (1976), *reprinted in* 1976 U.S.C.C.A.N. 3438, 3819.

This insightful look into the legislative history of the Social Security Act demonstrates that Congress understands unequivocally the importance of protecting the SSN and intended to make clear for future guidance that the words "for any other purpose," included in the language of the Act, mean precisely what they say. Courts have reached similar conclusions regarding the legislative intent behind the words "for any other purpose." *See United States v. Silva-Chavez*, 888 F.2d 1481 (5th Cir. 1989).

In 1981 Congress again amended 42 U.S.C. § 408, changing the offense from a misdemeanor to a felony and adding the language "or for the purpose of obtaining anything of value from any person" before "or for any other purpose." *See* Omnibus Reconciliation Act, Pub. L. No. 97-123, § 4, 95 Stat. 1659, 1663-64 (1981). While the House Conference Report accompanying the amendment offers no explanation of the reasons for the change (*see* H.R. CONF. REP. NO. 97- 409 (1981), *reprinted in* 1981 U.S.C.C.A.N. 2681, 2687-88), the text of the amendment makes clear Congress' intent both to punish a broader range of acts and to impose a stiffer penalty for misuse of the SSN. In summing up the prior law the House Conference Report stated:

> Criminal penalties are provided for: (1) knowingly and willfully using a social security number that was obtained with false information, (2) using someone else's social security number, or (3) unlawfully disclosing or compelling the disclosure of someone else's social security number.

See H.R. CONF. REP. NO. 97-409 (1981), *reprinted in* 1981 U.S.C.C.A.N. 2681, 2687.

D. The Identity Theft and Assumption Deterrence Act of 1998

In 1998 Congress passed the Identity Theft and Assumption Deterrence Act (Identity Theft Act), Pub. L. No. 105-318, 112 Stat. 3007 (1998), which created a new offense of identity theft. *See* 18 U.S.C. § 1028(a)(7). Prior to enactment of the Identity Theft Act, the statute (18 U.S.C. § 1028) addressed only the fraudulent creation, use, or transfer of identification documents and did not address the theft or criminal use of an individual's personal information. The new Identity Theft Act was enacted by Congress with two purposes in mind: to expand the scope of 18 U.S.C. § 1028(a) which, prior to the Identity Theft Act, made identification document fraud a criminal offense, and with enactment of the 1998 legislation made "the unlawful transfer and use of identity information" a criminal offense as well; and to legally recognize the individual as a victim of identity theft, establishing their rights to restitution. The law, in addition, established an educational and complaint service for individual victims at the Federal Trade Commission. *See* S. REP NO. 105-274 (1998). In meeting its intended purpose, the new law made it a crime to obtain SSNs, birth dates, and birth certificates without authorization and with the intent to commit fraud. *Id*. Also, the law made it a crime to aid or abet any unlawful activity that constituted a violation of federal law, or that constituted a felony "under any applicable State or local law." *Id*. Specifically, § 1028(a)(7) provides that it is unlawful for anyone who:

> knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law....

See 18 U.S.C. § 1028(a)(7).

Before passage of the 1998 act, the unauthorized use or transfer of identity documents was illegal under 18 U.S.C. § 1028, which included subsections (a)(1) through (a)(6). The unauthorized use of credit cards, personal identification numbers, automated teller machine codes, and other electronic access devices was illegal under another section of the U.S. Code, that is, 18 U.S.C. § 1029 ("fraud and related activity in connection with access devices"). The addition of subsection (a)(7) to § 1028 expanded the definition of "means of identification" to include such information as SSN and other government identification numbers, dates of birth, and unique biometric data (e.g., fingerprints), as well as electronic access devices and routing codes used in the financial and telecommunications sectors. Under the Identity Theft Act, the new definition of means of identification included prior statutory definitions of "identification documents."

The Identity Theft Act was clearly intended by Congress to cover a variety of individual identification information, including the SSN, that may be used by thieves to commit identity theft crimes. The Identity Theft Act, for example, amended § 1028(d)(3) to define "means of identification," as used in § 1028(a)(7), to include "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual." Several specific examples were listed in the Identity Theft Act, including name, SSN, date of birth, government issued driver's license, and other numbers; unique biometric data, such as fingerprints, voice print, retina or iris image, or other physical representation; unique electronic identification numbers; and telecommunication identifying information or access devices. In addition, the Identity Theft Act also modified the definition of "document-making implement," included in § 1028(d)(1), to include computers and software specifically configured or primarily used for making identity documents.

A key impact intended by the Identity Theft Act was to "make the proscriptions of the new identity theft law applicable to a wide range of offense conduct, which can be independently prosecuted under numerous existing statutes." *See Economic Crimes Policy Team, Identity Theft Final Report* U.S. SENTENCING COMMISSION REP. (1999), *available at* http://www.ussc.gov/identity/identity.htm. Thus, after enactment of the Identity

Theft Act, any unauthorized use of any means of identification could be charged either as a violation of the new law or in conjunction with other federal statutes.

E. Internet False Identification Prevention Act of 2000

In December 2000 Congress passed the Internet False Identification Act of 2000 (IFIA), which amended the False Identification Crime Control Act of 1982 (*see* False Identification Crime Control Act of 1982, Pub. L. No. 97-398, 96 Stat. 2009 (codified as amended at 18 U.S.C. § 1028 (1998)) to include computer-aided false identity crimes. *See* Internet False Identification Act of 2000, Pub. L. No. 106-578, 114 Stat. 3075 (2000). Specifically, the IFIA amended existing federal criminal law on identity theft, as it related to false identification, to include computer templates, files, and discs in the definition of "document-making implement" under 18 U.S.C. § 1028(d)(1), which already prohibited the transfer of a document-making implement with the intent that it would be used to produce a false identification document (such as a counterfeit Social Security card). In addition, the IFIA clarified that sale or distribution of false identification documents through computer files or computer templates is illegal. The IFIA specifically included the transfer of a false identification document by electronic means as part of prohibited conduct under 18 U.S.C. § 1028 and also prohibited placing a template for making false identifications on a Web site or other online location available to others. The result is that enactment of the IFIA made it easier to prosecute those who manufacture, distribute, or sell counterfeit identification documents.

F. Identity Theft Penalty Enhancement Act

The Identity Theft Penalty Enhancement Act of 2004 (ITPEA) was signed into law by President Bush on July 15, 2004. *See* Pub. L. No. 108-275; 18 U.S.C. § 1028A. The ITPEA requires mandatory imprisonment for those convicted of knowingly transferring, possessing, or using, without lawful authority, a means of identification of another person. *See* 18 U.S.C. § 1028A(a)(1). The mandatory minimum for the offense is two years (*See* § 1028A(a)(1)) and can go as high as five years if the theft is in connection with a terrorist act, such as offenses relating to aircraft destruction or tampering, use of explosives, and killing or attempting to kill during attacks on federal facilities. *See* § 1028A(a)(2). In addition, probation for conviction under this section is prohibited. *See* § 1028A(b)(1). The inclusion of possession of such materials makes this crime applicable to individuals and companies who use the internet and e-mail to unknowingly obtain personal information such as Social Security Numbers by claiming to be a financial institution. This scheme, known as "phishing," allows individuals or groups to obtain identifying information and use it to obtain other personal information and to secure things such as credit cards and loans in the victim's name. Previous acts prohibited obtaining this information to transfer it to others, but did not prohibit possession (18 U.S.C. § 1028(a)). The ITPEA now makes it possible to charge those who possess and use the information, in addition to those who transfer it, and also adds possession to the statute that addresses fraud and related activity in connection with identification documents. 18 U.S.C. § 1028 (a)(7). The statute prohibits knowing transfer, possession, or use of another's identification, without permission, with the intent to commit, aid, or abet a crime. The imprisonment term is also increased from three years to five years for an offense. ITPEA also requested that the United States Sentencing Commission review and amend existing guidelines to "appropriately punish identity theft offenses involving an abuse of position." Specifically, the ITPEA directed the Sentencing Commission to amend U.S.S.G. 3B1.3 to include instances in which an individual exceeded or abused his authority with regard to another's identity.

III. Statutory authority for prosecuting SSN misuse and identity theft

A. The statutory framework of 42 U.S.C. § 408(a)(7)(A)-(C)

In 1981 Congress amended the misdemeanor provisions of the Act, making Social Security fraud (including SSN misuse) a felony, punishable by five years in prison and a fine up to $5,000. *See* Omnibus Reconciliation Act, Pub. L. No. 97-123, § 4, 95 Stat. 1659, 1663-64 (1981); *see also* 42 U.S.C. §§ 408(a)(7)(A)-(C). The Social Security Act's primary criminal provisions relating to misuse of a Social Security Number

(§§ 408(a)(7)(A)-(C)), are set forth below in pertinent part:

> In general
>
> Whoever–
>
> (7) for the purpose of causing an increase in any payment authorized under this subchapter (or any other program financed in whole or in part from federal funds), or for the purpose of causing a payment under this subchapter (or any such other program) to be made when no payment is authorized thereunder, or for the purpose of obtaining (for himself or any other person) any payment or any other benefit to which he (or such other person) is not entitled, or for the purpose of obtaining anything of value from any person, or for any other purpose
>
> (A) willfully, knowingly, and with intent to deceive, uses a social security account number, assigned by the Commissioner of Social Security (in the exercise of the Commissioner's authority under § 405(c)(2)(A) of this title to establish and maintain records) on the basis of false information furnished to the Commissioner of Social Security by him or by any other person;
>
> (B) with intent to deceive, falsely represents a number to be the social security account number assigned by the Commissioner of Social Security to him or to another person, when in fact such number is not the social security account number assigned by the Commissioner of Social Security to him or to such other person;
>
> (C) knowingly alters a social security card issued by the Commissioner of Social Security, buys or sells a card that is, or purports to be, a card so issued, counterfeits a social security card, or possesses a social security card or counterfeit social security card with intent to sell or alter it."

See 42 U.S.C. §§ 408(a)(7)(A)-(C).

B. The statutory framework of 18 U.S.C. § 1028(a)(7)

The Identity Theft Act, 18 U.S.C. § 1028(a)(7), makes it a federal crime for anyone to knowingly transfer or use, in or affecting interstate or foreign commerce, (or cause to be transported in the mail in the course of the transfer or use) without lawful authority, a means of identification of another person, with the intent to commit, or to aid and abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law.

C. The statutory framework of 18 U.S.C. § 1028A

The ITPEA creates mandatory imprisonment for a term of two years for those convicted of knowingly transferring, possessing, or using, without lawful authority, a means of identification of another person. The primary criminal provisions of the Identity Theft Penalty Enhancement Act (ITPEA) relating to misuse of a Social Security Number is 18 U.S.C. § 1028A.

Title 18 U.S.C. § 1028A(b), concerning sentencing, reads as follows:

> (b) Consecutive sentence.--Notwithstanding any other provision of law--
>
> (1) a court shall not place on probation any person convicted of a violation of this section;
>
> (2) except as provided in paragraph (4), no term of imprisonment imposed on a person under this section shall run concurrently with any other term of imprisonment imposed on the person under any other provision of law, including any term of imprisonment imposed for the felony during which the means of identification was transferred, possessed, or used;
>
> (3) in determining any term of imprisonment to be imposed for the felony during which the means of identification was transferred, possessed, or used, a court shall not in any way reduce the term to be imposed for such crime so as to compensate for, or otherwise take into account, any separate term of imprisonment imposed or to be imposed for a violation of this section . . . .

IV. Charging decisions for SSN misuse and identity theft prosecutions

A. Charging SSN misuse using Title 42 of the Social Security Act

The felony provisions of 42 U.S.C. § 408(a)(7)(A)-(C), which deal with the misuse of an SSN, are particularly effective in charging cases involving identity theft or the attempt to manipulate the identification systems currently in place, or where an individual has entered the country illegally. In many cases recipients of Social Security benefits under one Title II program will be caught using a false identity and SSN to apply for, and collect, benefits under a second (or the same) Title II benefit program. This has been a common technique used by criminal travelers, who use multiple identities to apply for, and collect, benefits from SSA offices in different regions of the country.

The elements of proof for each subsection of § 408(a)(7) are more flexible than those required by 18 U.S.C. § 1028, a better known identity theft statute, that also contains subsections dealing with the misuse of an SSN. What follows is a description of each of the three subsections of § 408(a)(7), including a breakdown of the elements necessary to prove a charge under each, and a brief suggestion of when and how each subsection should be charged.

The elements required to prove a violation of § 408(a)(7)(A) are: defendant,

- with intent to deceive;
- willfully and knowing uses a Social Security account number;
- assigned to him by the Commissioner of SSA;
- based on false information furnished by defendant or another person to the Commissioner of Social Security. *See* 42 U.S.C. § 408(a)(7)(A).

Any fraudulent use of an SSN, whether made-up by the offender or obtained on the basis of false information supplied to SSA, is actionable and constitutes a felony for purposes of § 408(a)(7)(A). For example, a subject in the United States on a tourist visa secures a non-work SSN using his French passport. The subject then uses an alias to file a bogus application for asylum, resulting in United States Citizenship and Immigration Services (USCIS) approval and issuance of a green card and alien registration number. The subject then uses his new name and illegally procured USCIS documents to apply for a second SSN, thus completing the creation of a new identity. The subject then uses the second SSN to secure credit cards, open bank accounts, attend flight training, and make applications for employment as a pilot. The subject's use of the SSN is actionable because he used false and fraudulent documents (deceptively procured from the USCIS) to deceive SSA into issuing him a new SSN, and he may be charged with a felony under § 408(a)(7)(A). *See United States v. Pryor*, 32 F.3d 1192, 1194 (7th Cir. 1994) (defendant acted "willfully, knowingly, and with intent to deceive," in illegally using an SSN obtained on basis of false information).

The elements required to prove a violation of § 408(a)(7)(B) are:

- false representation of a Social Security account number;
- with intent to deceive;
- for any purpose.

See United States v. Means, 133 F.3d 444, 447 (6th Cir. 1998) (setting forth the elements for prosecution of a case under 42 U.S.C. § 408(a)(7)(B)). *See also United States v. McCormick*, 72 F.3d 1404, 1406 (9th Cir. 1995).

The majority of jurisdictions apply the *Means* standard as set forth above. However, a few jurisdictions break down the language of § 408(a)(7)(B) to include a fourth element:

- for any purpose;
- with intent to deceive;
- represented a particular Social Security account number to be his;
- which representation is false.

See United States v. O'Brien, 878 F.2d 1546 (1st Cir. 1989).

Subsection (B) is the most commonly charged subsection of § 408(a)(7) because of its broad application and straightforward elements of proof. It is typically charged whenever a subject has misrepresented an SSN to open a bank account; apply for a credit card; secure credit for a cell phone; rent or lease an apartment or car; apply for employment; or enroll in flight training. The

charging standard, for any purpose, is broad and self-explanatory, and any false representation of an SSN, with an intent to deceive, is actionable conduct that may be charged as a felony under § 408(a)(7)(B). *See United States Silva-Chavez*, 888 F.2d 1481 (5th Cir. 1989).

Direct evidence is not always necessary in order to prove that a defendant intended to use a Social Security card or number for deceptive purposes. Mere possession of a Social Security card or number that does not belong to a defendant is sometimes sufficient to support a finding that the defendant intended to deceive. *United States v. Charles*, 949 F.Supp. 365 (D. VI 1996). In *Charles*, the government was unable to produce direct evidence that the defendant had actually applied for a driver's license using a false SSN. Nevertheless, the jury could infer that the defendant received the Social Security card through false representations when the government's evidence showed that the Police Department Licensing Section had printed defendant's license; and generally, in order to obtain such a license, an applicant must give an SSN to the licensing agent.

Mere possession, however, of false identity documents, including a false SSN, might not always be enough to convict. Some courts have held that the term "represent" connotes a positive action, not merely passive possession, and have thus reasoned that Congress, by using the term "represent," meant to proscribe the "use," not merely the "possession," of a false SSN. *United States v. McKnight*, 17 F.3d 1139, 1144-45 (8th Cir. 1994). The concurring opinions of two *McKnight* panel members, however, indicate that this is not a hard and fast rule.

> We write separately to make explicit that possession of an identification card bearing a false social security number can, in some instances, provide a sufficient predicate for a jury to properly infer that a defendant falsely represented a social security number in violation of 42 U.S.C. § 408(a)(7)(B).

Id. at 1146; See also *United States v. Teitloff*, 55 F.3d 391, 394 (8th Cir. 1995), where the court rejected the defendant's contention that he did not technically "use" the SSN because the DMV computer system automatically provided that information when he supplied the other person's identification documents.

A defendant may be found to have acted willfully, knowingly, and with intent to deceive, even if the defendant did not intend to deceive federal officials when he presented them with documents containing a false SSN. See *Pryor*, 32 F.3d 1192, where the defendant's driver's license had been suspended and he was found to be carrying false documents which he acknowledged that he planned to present if pulled over for a traffic violation.

The Ninth Circuit has held that an alien's use of a false SSN to further otherwise legal conduct is not a crime of "moral turpitude." *Beltran-Tirado v. Immigration and Naturalization Serv.*, 213 F.3d 1179, 1184 (9th Cir. 2000). The significance of this decision lies in the impact such a conviction would have on the illegal alien's eligibility for inclusion on the Immigration and Nationality Act registry. *See* 8 U.S.C. § 1259. The registry statute was originally enacted by Congress in 1929 as a means to regularize the status of long-time illegal aliens residing in the United States, and has been updated periodically since. Under current registry provisions, conviction for a crime of moral turpitude would preclude an alien from eligibility because he would not be considered "of good moral character." *Id.*

In *Beltran-Tirado*, the defendant lived under an assumed identity, using the name and SSN of the victim to marry twice and obtain employment, a driver's license, credit cards, and a Housing and Urban Development loan. The defendant's earnings attracted the interest of the IRS, resulting in her arrest and conviction under 42 U.S.C. § 408(a)(7)(B) and 18 U.S.C. § 1546(b)(3). The INS moved to deport her, but the Ninth Circuit intervened to interpret the legislative history of 42 U.S.C. § 408 and carve out an exception to a conviction for a crime of moral turpitude by allowing the use of a false SSN to further "otherwise legal behavior." The *Beltran-Tirado* case appears consistent with an earlier decision by the Ninth Circuit in which the court concluded that

> the crime of knowingly and willfully making any false, fictitious or fraudulent statements or representations to an agency of the United States is not a crime of moral turpitude because a jury could convict if it found that the defendant had knowingly, but without evil intent, made a false but not fraudulent statement.

Hirsch v. INS, 308 F.2d 562, 567 (9th Cir. 1962).

Another California federal court, citing *Beltran-Tirado*, held that the sale of false or counterfeit SSNs is a crime that involves moral turpitude. *Souza v. Ashcroft*, No. C00-4246MMC, 2001 WL 823816 (N.D. Cal. July 16, 2001). The court distinguished between those who sell, rather than use, false or counterfeit Social Security cards ("persons convicted of the crime of selling false or counterfeit Social Security cards have, like persons convicted of the analogous crime of selling counterfeit green cards, committed a crime of moral turpitude"), *id.* at *3, and stated that Congress, in amending 42 U.S.C. § 408, specifically excluded from the exemption those who sell, rather than use, false or counterfeit Social Security cards. The reason for this distinction is apparent. Selling false alien registry documents (green cards), as well as selling false or counterfeit Social Security cards, inherently involves a deliberate deception of the government and an impairment of its lawful functions.

When an individual makes multiple false representations by misrepresenting an SSN on multiple credit card applications, bank accounts, or federal documents relating to employment (I-9, W-4 forms), that person may be charged with a separate offense for each use or representation. Each of the separate offenses is supportable by a different set of predicate facts and is actionable under § 408(a)(7)(B). In addition, each use or representation on a federal form is actionable as a false statement under 18 U.S.C. § 1001 and can be charged as a separate offense, also supportable by a different set of predicate facts. While charging multiple counts might not be desirable, doing so when separate predicate facts exist would not run afoul of the rule against multiplicity that prohibits the charging of a single offense in several counts. *United States v. Castaneda*, 9 F.3d 761, 765 (9th Cir. 1993) (holding that a defendant may properly be charged with committing the same offense more than once as long as each count depends on a different set of predicate facts); *see also United States v. Hurt*, 795 F.2d 765, 774-75 (9th Cir. 1986).

It is not necessary that the false use or representation of an SSN have a detrimental effect, in some way, on the government to be actionable. *See United States v. Holland*, 880 F.2d 1091 (9th Cir. 1989). Any use of a false SSN on nonfederal documents is still actionable under § 408(a)(7)(B). For example, an individual used his falsely obtained SSN when completing multiple applications seeking employment as a pilot and in applying for taxi permits with airport cab companies. Even though the airline and cab company employment applications are not federal documents, the subject can still be charged under § 408(a)(7)(B). Further, it is not necessary to prove that the defendant used a false SSN for payment, gain, or pecuniary value. *Silva-Chavez*, 888 F.2d 1481. In addition, the Fourth Circuit has held that § 408(g)(2) applies to private, purely commercial transactions. *United States v. Bales*, 813 F.2d 1289, 1297 (4th Cir.1987) (affirming convictions for using false SSN in seeking bank loans). *See United States v. Darrell*, 828 F.2d 644 (10th Cir. 1987). *See also United States v. Rosenberg*, 806 F.2d 1169, 1171-72 n. 1, 1180 (3d Cir.1986) (use of false SSN in a commercial transaction).

The use or nonuse of a defendant's SSN on loan applications and tax returns is not protected by the First Amendment. *See United States v. Bales*, 813 F.2d 1289 (4th Cir. 1987). Similarly, a defendant's deceitful use of another person's SSN to open a bank account was within the "any other purpose" clause of a statute prohibiting deceptive use of an SSN. *United States v. Barel*, 939 F.2d 26, 28 (3d Cir. 1991) ("The Social Security felony fraud statute applies to the intentional use of a false social security number 'for any purpose' when a defendant uses a false social security number to open bank accounts, even absent proof of pecuniary gain to defendant"). False representation of a fake, nonexistent SSN may constitute the offense of false pretenses. *See United States v. Bales*, 813 F.2d 1289 (4th Cir. 1987).

According to 18 U.S.C. § 1028(d)(1), an "identification document" is "a document made or issued by or under the authority of the United States Government...which, when completed with information concerning a particular individual, is of a type intended or commonly accepted for the purpose of identification of individuals." The House Report accompanying what became § 1028 demonstrates that the definition includes not only "identification documents, such as driver's licenses, which are widely accepted for a variety of identification purposes," but also those "'commonly accepted' in certain circles for identification purposes, such as identification cards issued by state universities and federal government identification cards." H.R.

REP. No. 802, 97th Cong.9 (1982), *reprinted in* 1982 U.S.C.C.A.N. 3519, 3527. The House Report also notes that identification documents "normally will include such identifying elements as an individual's name, address, date, or place of birth, physical characteristics, photograph, fingerprints, employer, or any unique number assigned to an individual by any federal or state government entity." *Id.*

Two published circuit court decisions, both by the Fourth Circuit, have applied the definition of "identification documents" under 18 U.S.C. § 1028. They involved Social Security cards and Form I-94 Arrival-Departure Records, which the courts concluded were "identification documents" within the meaning of the statute. *See United States v. Pahlavani*, 802 F.2d 1505 (4th Cir.1986) (I- 94 forms). In *United States v. Quinteros*, 769 F.2d 968 (4th Cir. 1985), the court relied on testimony that Social Security cards were "commonly accepted" as identification documents. An employee of the Social Security Administration testified that the Administration often issued cards for older persons to use as identification for cashing checks. She also testified that because the cards were so often used for identification, the government removed a notice from the back of the cards that stated "Not for Identification Purposes." In all, the court concluded, there was a "common understanding that Social Security cards are identification documents." Id. at 970.

In *United States v. McGauley*, 279 F.3d 62 (1st Cir. 2002), the defendant was charged with making false statements to the U.S. Postal Service, in violation of 18 U.S.C. § 1001; misrepresentation of SSNs, in violation of 42 U.S.C. § 408(a)(7)(B); mail fraud, in violation of 18 U.S.C. § 1341; and money laundering, in violation of 18 U.S.C. § 1956(a)(1)(B)(i). The court held that convictions for five counts of misrepresentation of SSNs were supported by evidence that the defendant had used false numbers to open post office boxes under names other than her own, and had refund checks she fraudulently obtained from retail stores sent to those post office boxes. The court also found that the Social Security statute, which proscribes the use, with intent to deceive, of a false SSN, did not require that the SSN be used for the purpose of obtaining a payment to which the user was not entitled.

Use of a false SSN in a debtor's joint petition resulted in dismissal of the case for cause under 11 U.S.C.A. § 707(a). *In re Riccardo*, No. 99 B 12036 ASH, 2000 WL 692466 (Bankr. S.D.N.Y. May 25, 2000). The court held that "use of false SSNs in debtors' petitions and notices of case commencement has become an all too prevalent and pernicious practice," and "(f)alsification of social security numbers is a species of fraud, specifically that of identity fraud, which threatens to undermine the integrity of the bankruptcy process." *Id.* at *1.

In *United States v. Tedder*, 81 F.3d 549 (5th Cir. 1996), the amount of loss considered in sentencing the defendant who pleaded guilty to fraudulent use of an SSN and aiding and abetting was properly calculated based on intended loss in the amount of loans applied for, rather than actual loss. The court reasoned that the purpose of the scheme was for the defendant's clients to obtain the full amounts of the loans applied for, and evidence did not show that defendant had any control over repayment.

The use of SSNs as identifiers in a great range of transactions in today's society is so prevalent that Congress included false use "for any reason" within the scope of acts prohibited under § 408(a)(7). Section 408(a)(7)(B) provides that whoever—for the purpose of obtaining anything of value from any person, or "for any other purpose"

> with intent to deceive, falsely represents a number to be the Social Security account number assigned by the commissioner of Social Security to him or to another person, when in fact such number is not the Social Security account number assigned by the commissioner of Social Security to him or to such other person. . . shall be guilty of a felony and upon conviction thereof shall be fined under Title 18 or imprisoned for not more than five years, or both.

The statute therefore requires that an identity thief actually represent the false Social Security Number to another. The term "represent" connotes a positive action, not merely passive possession. Indeed, the legislative history and legislative intent of § 408 reflects Congress' principal concern with forbidding the use of a fraudulent number. The statutory language and the legislative history of § 408(a)(7)(B) indicate, however, that Congress was interested in proscribing the use of

a false Social Security Number, not just mere possession of a false number. *See McKnight*, 17 F.3d 1139. The advantage to proceeding under Title 42, when the facts or law merit such a pleading, is that "for any other purpose" is broadly defined because the legislative intent of the law is plainly to proscribe the misuse of SSNs. A defendant's deceitful use of a false SSN to open a bank account is within the "for any other purpose" clause. *See Barel*, 939 F.2d at 34. Another benefit of the statute is that the phrase "with the intent to deceive" does not require the intent to deceive the government. *See Holland*, 880 F.2d at 1095. Also, the statute does not require that a defendant possess the motive of pecuniary gain. *See United States v. Johnson-Wilder*, 29 F.3d 1100, 1103 (7th Cir. 1994). Significantly, there are circumstances when an identity thief has an "intent to deceive" under 42 U.S.C. § 408(a)(7)(B), but does not have the intent to commit any unlawful activity that would constitute a violation of federal, state, or local law, as outlined in 18 U.S.C. § 1028(a)(7). Therefore, it is absolutely essential that federal prosecutors have a choice of statutes under which to charge someone with identity theft.

The elements required to prove a violation of 42 U.S.C. § 408(a)(7)(C) are:

- defendant knowingly alters a Social Security card; or
- defendant counterfeits or possesses a Social Security card with intent to sell or alter it;
- or defendant buys or sells a Social Security card.

This subsection is typically charged when a subject has knowingly altered a Social Security card (usually to remove work restrictions from the face of the card), or has manufactured or counterfeited a card or cards for sale on the black market. This section can also be charged when an individual is discovered to have purchased a Social Security card for his own use or for resale. The altered and/or counterfeited cards are then used to secure false identification documents, open bank accounts, apply for credit cards, and to work, including employment in sensitive positions at airports, government facilities, and other locations requiring security clearances.

To pass as a counterfeit, an image must bear such a likeness to the original as "is calculated to deceive an honest, sensible, and unsuspecting person of ordinary observation and care dealing with a person supposed to be upright and honest." *United States v. Gomes*, 969 F.2d 1290, 1293 (1st Cir. 1992). To qualify as counterfeit, a bogus copy of a Social Security card does not have to be such a good imitation that it baffles an expert. *Id.* at 1294.

B. Charging SSN misuse using the Title 18 Identity Theft Statutes

The elements required to prove a violation of 18 U.S.C. § 1028(a)(7) are:

- that the defendant knowingly transferred or used, without lawful authority, a means of identification of another person;
- that the defendant so acted with the intent to commit, or to aid and abet, unlawful activity that constitutes a violation of federal law (or a state or local felony); and
- that the defendant's transfer or use, was in, or affected, interstate or foreign commerce (or the means of identification was transported in the mail in the course of the transfer or use).

Under 18 U.S.C. § 1028(a)(7), "means of identification" does not require the production, possession, or use of an actual identification document. Instead, "means of identification" is broadly defined to include a wide range of personal identifying information. The definition includes any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any name, SSN, date of birth, official state or government-issued driver's license or identification number, alien registration number, government passport number, or employer or taxpayer identification number.

The elements required to prove a violation of 18 U.S.C. § 1028A are:

- defendant committed the crime of [Conspiracy to Commit Bank Fraud, Conspiracy to Possess Fifteen or More Unauthorized Access Devices, or Possession of Fifteen or More Unauthorized Access Devices] as charged in the indictment;
- defendant knowingly [transferred], [possessed], or [used], without lawful authority, a means of identification of another person; and

- defendant transferred, possessed, or used a means of identification during and in relation to the crime.

V. Sample indictments

The following are samples of Indictments of SSA fraud using the Title II felony fraud provisions.

1. 42 U.S.C. § 408(a)(7)(A)

COUNT _____

[42 U.S.C. § 408(a)(7)(A)]

On or about _____, in Los Angeles County, within the Central District of California, defendant _____, aka _____, in a matter within the jurisdiction of the Social Security Administration, did willfully, knowingly, and with the intent to deceive and obtain a thing of value, use Social Security Number XXX-XX-XXXX, assigned to defendant by the Commissioner of Social Security, having obtained that Social Security Account Number on the basis of false information furnished by defendant to the Commissioner of Social Security. Specifically, defendant used Social Security Number XXX-XX-XXXX on a Statement for Determining Continuing Eligibility for SSI (SSA Form 8202-F6) to obtain Social Security benefits payments, knowing that said number had been obtained through his submission of an application to the Commissioner of Social Security for a second Social Security Number, in which he had falsely denied that he had previously applied for and been granted another Social Security Number.

2. 42 U.S.C. § 408(a)(7)(B)

COUNT _____

[42 U.S.C. § 408(a)(7)(B)]

On or about March 14, 2000, in Los Angeles County, within the Central District of California, defendant _____, for the purpose of obtaining something of value and for other purposes, and with the intent to deceive, falsely represented on an application for employment with _____, that XXX-XX-XXXX was the Social Security Number assigned to him by the Commissioner of Social Security, when in fact, as he well knew, such number was not the Social Security Number assigned to him by the Commissioner.

3. 42 U.S.C. § 408(a)(7)(C)

COUNT _____

[42 U.S.C. § 408(a)(7)(C)]

On or about March 13, 2001, in Los Angeles County, within the Central District of California, defendant _____, knowingly possessed and intentionally used an altered, purchased, or counterfeited Social Security Number card, XXX-XX-XXXX, for the purpose of obtaining something of value and for other purposes. Specifically, defendant used a counterfeited Social Security card and Social Security Number XXX-XX-XXXX as proof of identification when completing an application and I-9 and W-4 forms to secure employment with _____.

4. 18 U.S.C. § 1028(a)(7)

COUNT _____

[18 U.S.C. § 1028(a)(7)]

On or about _____, in the Central District of California and elsewhere, defendants _____ and _____, in connection with an application for an extension of credit from _____ Financial Corporation, Los Angeles, California, knowingly used and attempted to use, without lawful authority, in and affecting interstate commerce, a means of identification of another person, that is certain eight digit numbers assigned to ____ and ____ as their Social Security Numbers, with the intent to commit unlawful activity in violation of federal law, that is mail fraud, in violation of Title 18, United States Code Section 1341, and by such conduct the defendants obtained items of value aggregating $1,000 or more during a one-year period.

5. 18 U.S.C. § 1028A

COUNT _____

[18 U.S.C. § 1028A]

On or about _____, in Los Angeles County, within the Central District of California, defendants _____ and _____ knowingly transferred, possessed, and used, without lawful authority, a means of identification of another person, that is, approximately, fifteen (15) or more credit card account numbers assigned to other persons, four (4) or more checking accounts assigned to other persons, and three (3) or more savings account numbers assigned to other persons, during and in relation to the following felonies: (a) Conspiracy to Commit Bank Fraud, a violation of Title 18, United States Code, Section

1349, as charged in Count One; (b) Conspiracy to Possess at Least Fifteen (15) Counterfeit and Unauthorized Access Devices, a violation of Title 18, United States Code, Section 1029(b), as charged in Count Two; and (c) Possession of Fifteen (15) or More Counterfeit and Unauthorized Access Devices, in violation of Title 18, United States Code, Section 1029(a)(3), as charged in Count Three, and further did aid, abet, counsel, command, induce, procure and cause another to do the same.

VI. Conclusion

Identity theft was clearly identified by Congress as a serious crime when the Identity Theft Act was passed in 1998 and when the Social Security Act was amended to make misuse of a Social Security Number a felony. Since then, law enforcement agencies at all levels, federal and nonfederal, have worked together to develop strategies for investigation and prosecution of offenders.❖

ABOUT THE AUTHOR

❑**John K. Webb** is a Senior Attorney with the Office of Chief Counsel for the Inspector General, Social Security Administration, and a Special Assistant United States Attorney with the United States Attorney's office for the Central District of California, Los Angeles, where he serves as Identity Theft Coordinator. He is responsible for prosecuting federal crimes involving identity fraud and abuse of Social Security programs, and has participated in the indictment and prosecution of individuals related to the terror attacks of 9/11, as well as the planning and implementation of Operation Tarmac/Operation Safe Harbor in Phoenix and Los Angeles. Mr. Webb has served as an instructor at the National Advocacy Center and is a frequent lecturer on the topics of identity theft, Social Security Number misuse, and federal benefits fraud. Mr. Webb is a regular contributor to the *United States Attorneys' Bulletin*.✠

Using Electronic Evidence to Litigate Social Security Cases: Considering the Implications of the Social Security Administration's New Signature Alternatives on Applications

Joseph Grow
Staff Attorney
Office of Inspector General
Social Security Administration

I. Introduction: SSA's move toward electronic processes

This article will review three new alternate signature processes that the Social Security Administration (SSA) recently adopted, and it will describe SSA's paper-based procedures that will remain for documenting identity. The article will also review statutes traditionally used to litigate benefits fraud under the Social Security programs and will discuss anticipated legal challenges to SSA's new electronic signature processes. Finally, the article will emphasize the need for continued cooperation between SSA and the Department of Justice (Department) to address and meet these challenges.

SSA, the largest independent federal agency, administers the Social Security retirement, disability, and survivors insurance programs, paying $430 billion annually in benefits to almost forty-six million beneficiaries. It also administers the Supplemental Security Income (SSI) program that provides $31 billion in assistance to over six million people with limited income and assets. All of these payments can be traced back to a very important initial transaction—an application for benefits. This essential transaction, which can occur in a variety of mediums, has recently been the subject of an SSA redesign.

A. Migrating to a paper-free environment

In an effort to make the transition from the use of paper forms and files in its claims process to a completely electronic claims environment, SSA has invested in the conversion to an electronic application process which eliminates the storage of paper. With this aim, SSA plans to develop and implement a more efficient system that will enable its processing components to provide enhanced service to the public. Many of the disadvantages of a paper process are obvious:

- requires a lot of storage space;
- single documents may be easily lost;
- search capabilities and access to physical copies are limited; and
- paper deteriorates over time, in addition to being unwieldy and costly to transport.

These disadvantages often result in longer processing times for SSA and applicants, especially in the disability appeals process.

B. Paperwork Elimination Act

Besides the long processing times and inherent problems with a paper-based process, the trend of government-wide transition to electronic processes is motivated by the call for the expansion of electronic government services in the President's Management Agenda, as well as advancements in technology. To ease electronic transitions, the Government Paperwork Elimination Act (GPEA), 44 U.S.C. § 3504n (2003), requires agencies to provide for the use and acceptance of electronic signatures, and it also requires agencies to provide for the option of electronic maintenance, submission, or disclosure of information, when practicable, as a substitute for paper.

C. SSA regulations

Although not required by statute, SSA regulations require a signature for benefit applications. *See* 20 C.F.R. §§ 404.610, 416.310

(2003). Within the last decade, SSA has determined that applications do not need to be signed with a wet signature to be in accordance with the regulations. *See* SSA Ruling 96-10p (December 30, 1996) *available at* http://www.ssa.gov/OP_Home/rulings/oasi/33/SSR96-10-oasi-33.html. However, SSA has traditionally required a wet or "pen and ink" signature for its paper benefits applications. Therefore, when the Department litigated SSA cases, it relied on an individual's signature for purposes of identification and to show that the applicant verified the truth of the submitted information under penalty of perjury. Consequently, despite the disadvantages of paper, the paper-based system has some distinct advantages for the government litigator in Social Security cases because there are well-settled rules in litigation that address issues of the validity, authenticity, and reliability of paper documents, and alterations to documents can sometimes be more easily detected and proved through physical characteristics. *See, e.g.*, *Legal Considerations in Designing and Implementing Electronic Processes: A Guide for Federal Agencies* (November 2000) Sec. II.B.2., *available at* http://www.usdoj.gov/criminal/cybercrime/eprocess.htm. After such a long period of reliance on paper, it is reasonable to expect a transition period during which Assistant United States Attorneys (AUSAs) will need to familiarize themselves with the reliability of the new electronic processes in order to successfully present their Social Security cases.

II. Social Security's alternative signature processes on applications

A. Types of alternative signatures

SSA's new procedures for accepting alternatives to wet signatures which became effective June 21, 2004, are known as alternative signatures or "signature proxies." *See* 69 Fed. Reg. 24,699 (May 4, 2004) (publicizing the SSA ruling which announced the alternate means to satisfy the signing of SSA applications for benefits). There are three alternative signatures: "attestation" of interviewers for in-person and telephone interviews; "click and sign" for internet applications; and "witnessed signature" for paper applications with a wet signature. SSA will use these signature alternatives for initial applications for Retirement and Survivor's Insurance benefits, Disability Insurance Benefits, and SSI benefits. SSA plans to potentially extend its alternative signatures to other processes as it gains experience with their use on applications.

The following demonstrates more specifically how the alternative signatures will work. *See also* SSA's Program Operations Manual System (POMS) 00201.015, *available at* http://policy.ssa.gov/poms.nsf/poms.

B. Attestation of interviewers for in-person and telephone interviews

Many SSA applications take place via an in-person interview at an SSA field office or an interview over the telephone. The "attestation" process involves an SSA employee, usually a Claims Representative or a Teleservice Representative, electronically noting or attesting to an applicant's intent to sign and file an application, under penalty of perjury, that the information submitted is true. This electronically recorded annotation of the attestation will serve as an alternative to the wet signature which, in a majority of cases, provided the sole reason SSA had to retain the paper applications.

At the beginning of the in-person application process, an SSA interviewer informs an applicant that a wet signature is no longer required if he intends to file an application for benefits. Further, the SSA interviewer will ask the applicant whether he understands that the information the applicant provides will be used to process an application for benefits and the penalty for providing false information to SSA.

The SSA interviewer will continue with the interview, entering the applicant's responses into SSA's computer system, a practice that was used in the old process as well. Before concluding the interview, the interviewer will give the applicant a printed copy of the information the applicant provided in order to review the information and to confirm its accuracy.

In the final step of the interview, the interviewer will ask the applicant again if he understands that the information he gave SSA will be used to process an application for benefits. The interviewer will also ask the applicant to declare, under penalties of perjury, that the information is true and accurate to the best of his knowledge. The interviewer will give the applicant the information summary sheet for the applicant's

records, along with a cover notice reiterating the penalty of perjury language and stating the applicant's reporting responsibilities if the provided information changes.

The SSA interviewer will then attest to:

- the applicant's intention to file;
- the applicant's affirmation under penalty of perjury that the information the applicant provided is correct; and
- the applicant's agreement to "sign" the application for benefits, by annotating the applicant's agreement in the electronic claims record on SSA's computer system.

The SSA employee's attestation will serve to document the applicant's affirmation and "signing" of the electronic claim. SSA will consider this electronic application a valid application for benefits, which it will deem as signed and equivalent to a wet signature on a paper application.

In a telephone interview, the procedure will be the same as the in-person interview, except that SSA will mail the summary information sheet to the applicant. During the interview, the SSA interviewer will advise the applicant to review the mailed material and contact SSA within ten days if he needs to make any corrections. When the applicant receives the summary sheet, a cover notice will reiterate the penalty of perjury language and state the applicant's reporting responsibilities if the provided information changes. Consequently, SSA's procedures require repeated notification to the applicant (one verbal and one written) of the penalties for providing false information to the SSA, as well as the applicant's duty to notify SSA if any information changes in the future.

C. Witnesses signature for mailed or in-person applications

The "witnessed signature" procedure entails an SSA employee annotating the SSA's computer system when SSA receives a paper application with a wet signature. SSA does not expect this situation to occur often, but does anticipate its occurrence when an applicant insists on signing an application. SSA will not refuse these completed and signed applications. Instead, SSA employees will electronically record their attestation to the fact that they received a paper application with a wet signature under a penalty clause certification. SSA will deem this electronic annotation as the equivalent of a wet signature. SSA will return the paper application to the claimant along with a cover notice that includes reporting responsibilities and a claim receipt.

D. Click and sign for Internet claims

SSA will no longer require applicants filing for benefits using the Internet to print and sign the completed application and return it to SSA for processing. SSA has now approved the use of a "Click and Sign" electronic signature for individuals who file applications via the Internet at the SSA Web site. Applicants will be able to review their entries as they complete the application, and they will be able to review a summary page at the end of the process that displays all of the information provided.

At the conclusion of the Internet application, the applicant will establish the fact that he or she is filing for benefits, affirm the truthfulness of the information on his application, and agree to sign the electronic application for benefits by pressing a "sign now" button on the Internet screen. SSA will consider the application signed when the applicant submits it. A toll free number is provided if claimants decide they do not want to submit their application electronically.

E. Corroboration of identity

In connection with all of these electronic processes, SSA will continue to require evidence of the identity of the applicant prior to the final acceptance of all benefit applications and subsequent transactions. This will be achieved by continuing to require the applicant to provide some knowledge-based information to establish his identity which matches information contained in SSA's existing records. In addition, SSA will continue to require documentary evidence in the claims process. *See* SSA POMS sections GN 00201.015J; GN 00301, General Evidentiary Standards. For example, SSA often requires submission of a certified copy of a birth certificate. However, SSA will not retain this evidence in paper form. *See* SSA POMS sec. GN 00301.286, Electronic Evidence Documentation and Retention. Nevertheless, the SSA claims representatives will electronically document what was examined. *Id.* If medical records are required for a disability claim, the submission will occur at

a later stage and the records will help corroborate identity, as well as the validity of the claim.

III. Litigating Social Security cases

A. How the government has traditionally relied on evidence containing wet signatures in Social Security cases prior to alternative signature processes

The outcome of Social Security litigation involving fraudulent applications can dictate whether SSA may recover money that is owed from overpayment of benefits, hold applicants responsible for making statements to SSA that they knew or should have known were false, and deter future applicants from making false statements to SSA. It is important to remember that relatively small transactions that take place in great volume, such as applications for benefits, have the overall potential to expose SSA to significant risk.

Applications for government entitlements, the common denominator in the initiation of all benefits that SSA pays, are susceptible to fraud and litigation. *See e.g.*, *Supplemental Security Income: Long-Standing Problems Put Program at Risk for Fraud, Waste, and Abuse: Hearing before the Subcommittee on Oversight, House Comm. on Ways and Means,* 105th Cong. 97-98 (1997) (statement of Jane L. Ross, Director Income Security Issues, U.S. General Accounting Office) (SSI program has had significant problems in determining claimants' initial financial eligibility because of reliance on inaccurate accounts of individuals' own reports of their income and resources.). *See also Legal Considerations in Designing and Implementing Electronic Processes: A Guide for Federal Agencies* at sec. III.B.1. Therefore, the Department has had extensive experience in litigating Social Security cases involving applications that contain false statements, particularly on applications for disability benefits.

A material false statement on an application with a wet signature is generally considered a persuasive piece of evidence when litigating Social Security cases. AUSAs have traditionally used the wet signatures on applications to sufficiently identify the applicant who signed a document containing a false statement; to prove that the applicant read, and was familiar with, the false statement in the document; or had the opportunity to read it before it was signed; and that the applicant agreed and intended to be bound by the assertions contained in the document. In addition, the wet signature affirmed the accuracy of the information provided and an understanding of the obligations. *See e.g*, *Id.* at sec. II.B.2. It is important that the new alternative signatures serve as effective evidence because, without a credible deterrent to fraud through vigorous detection and prosecution policies, fraud may dramatically increase.

A list of sample legal provisions that the Department has traditionally used in Social Security cases where a paper application, containing a material false statement and wet signature, has been an important and persuasive piece of evidence are:

- 18 U.S.C. § 1001, Fraud and False Statements. This statute prohibits the knowing and willing falsification or concealment of any material fact, or the making of any false or fraudulent statement, including any false document or writing, in any matter within the jurisdiction of any department or agency of the United States. It is not necessary, for purposes of this statute, that the false statement be made in order to procure money or some other benefit. In 2003 there were 321 convictions of this charge involving the Social Security programs.
- 42 U.S.C. § 408, Social Security Penalties. This statute contains the Social Security Act's primary criminal provisions rendering it a felony to make, among other acts, false statements or misrepresentations as to material facts in applications for benefits under Title II of the Social Security Act. In 2003 there were 541 convictions of this charge for theft of SSA funds.
- 42 U.S.C. § 1383a, Fraudulent acts; penalties; restitution. This statute contains the criminal provisions for SSI fraud, including when an applicant knowingly and willfully makes, or causes to be made, any false statement or representation of a material fact in any application for SSI benefits. There were sixty-eight convictions of this charge in 2003.
- 18 U.S.C. § 641, Embezzlement and Theft: public money, property, or records. This statute prohibits stealing, including the theft of Social Security benefits, from the government, as well as receiving, concealing,

or retaining the stolen property with the intent to keep, use, sell, or otherwise convert it. In 2003 there were 321 convictions of this charge involving the Social Security programs; and

- 31 U.S.C. § 3729, False claims. This statute provides for the imposition of civil penalties for false claims made against the government. The most common application of this statute to Social Security would be cases in which the Department determines to pursue a civil, rather than criminal, action against an individual for making a claim for Social Security benefits which contains information that the individual knows to be false or which omits material facts.

B. Anticipated legal challenges with the new Social Security applications containing alternative signatures

The Department expects that agencies will exercise discretion in determining how to convert to electronic processes. Therefore, it is up to each agency to assess its own transactions and programs to determine what characteristics should be built into its electronic processes. *See Legal Considerations in Designing and Implementing Electronic Processes: A Guide for Federal Agencies* at sec. III.C. Although the Department did not develop these electronic processes, SSA has stated it will continue to work with the Department, an important stakeholder, to address any impairments to the Department's enforcement of the law that could arise with the new alternative signature processes.

Reliability of evidence will be an important future test as SSA's alternative signature processes will begin replacing wet signatures in legal challenges. AUSAs will soon be ascertaining whether SSA's attestation process will be sufficiently reliable to satisfy courts and others who must determine the facts surrounding agency actions. Future cases will reveal whether SSA's collection and maintenance of electronic records satisfy admission requirements and whether SSA preserves sufficient context and evidence of the process so that the new alternative signature records are effective in litigation.

For example, the GPEA provides that certain electronic signatures, maintained in accord with the Office of Management and Budget Guidance, shall not be denied legal effect, validity, or enforceability because they are in electronic form. However, GPEA does not require courts to accept electronic records and signatures that are deficient in other respects merely because they are in electronic form. GPEA defines "electronic signature" as "a method of signing an electronic message that (A) identifies and authenticates a particular person as the source of the electronic message; and (B) indicates such person's approval of the information contained in the electronic message." 44 U.S.C. § 3504. Therefore, a court might decline to give effect to electronic signatures that do not technically meet this definition.

The Department has recommended that agencies ensure that the electronic signature technologies adopted identify the signers of the document and demonstrate their intent and familiarity with the document. *See Legal Considerations in Designing and Implementing Electronic Processes: A Guide for Federal Agencies* at sec. II.B.2. It will be equally important for the SSA's new process to identify and authenticate government employees who act on or approve claims or transactions, and to record all pertinent information about their actions. *See id.*, n. 7. The SSA should be able to associate employees with electronic transactions through a PIN/password system that was also used during the paper application process.

The SSA expects that, in the event there is a court action challenging the application or signature, the SSA interviewer who attests to the applicant's signature should not have to appear in court. If the application is challenged, SSA anticipates proving "signing" through an SSA management official's testimony about SSA's signature alternative processes and procedures. Therefore, it appears critical that SSA follow consistent written policies and procedures pertaining to the alternative signature processes and make witnesses available to testify about the processes in Social Security fraud litigation. For exhibit purposes, computer printouts of the new application transactions should clearly associate interview questions with the applicant's responses.

The following are hypothetical examples to illustrate some of the safeguards that exist in the new processes and also some evidentiary issues that may need to be resolved.

Example 1: An applicant mails SSA his application for disability insurance benefits which contains material false statements. Specifically, he falsely represents his wages as being significantly less than they actually are in order to wrongfully obtain benefits. An SSA employee processes this application according to the "witnessed signature" alternative signature process. Later, in a prosecution pursuant to 42 U.S.C. § 408, the applicant claims that he qualified his responses with a handwritten note, mailed with his application, that explained he subtracted several expenses to compute the amount of wages he reported.

SSA will need to clarify whether it will make handwritten notes that qualify interview questions part of the paperless application. In addition, although SSA has no current plans to save paper applications now that its record schedule has been modified to accept media neutral records as the official agency record, SSA should consider retaining paper-based information in important or sensitive contexts. For example, SSA should save and refer any handwritten note containing indications of fraud to the Office of Inspector General for possible investigation.

Example 2: An applicant provides material false statements on an Internet "click and sign" application. Specifically he states that he has never before filed for benefits under any other name or SSN, and has never used any SSN or name other than his own. He then receives several years of disability benefits for which he is not eligible. In a false statement prosecution under 18 U.S.C. § 1001, he claims that he submitted truthful information on the Internet application but that someone at SSA must have altered it after he sent it.

This scenario illustrates a need for SSA to reliably document all alterations to applications after receipt so that AUSAs can prove that SSA did not alter the application. *See Legal Considerations in Designing and Implementing Electronic Processes: A Guide for Federal Agencies* at sec. III.C.1. It would also be beneficial to have the applicant affirm the truth of the statements each time an applicant provides new information to SSA or changes the information. *Id.* at sec. III.C.2.c.

Example 3: An applicant using the "click and sign" process on the Internet says his daughter was only working on a draft application that she never meant to send and that she must have pushed the "enter" button by accident, thus unwittingly transmitting her proclaimed draft as if it were a real application. The "draft" contained false statements that the applicant was not working, and based on these statements, SSA paid the applicant benefits for several years by direct deposit into a joint account which the applicant claims he did not monitor. The government decides to bring a case against the daughter for making a false claim under 31 U.S.C. § 3729. The daughter claims the applicant committed the fraud.

- The AUSA may attack the "accidental submission" argument on two grounds. First, SSA's electronic process makes it difficult for an application to be transmitted by "mistake," as it requires the applicant to click "yes" after being shown a message that explains that, by doing so, the applicant is submitting a final application under penalty of perjury. Second, the AUSA may show that SSA readily provides a toll free telephone number for applicants to notify SSA when an application has been submitted in error.
- It may be a challenge to prove the identity of the person who purports to submit an application for Social Security benefits. Someone closely related to the applicant may be privy to all necessary identifying information. This same risk exists under the current paper-based process. However, electronic signature alternatives may increase this risk because they lack the forensics of a wet signature.
- In general, it will be important for SSA to determine the date and time an applicant submits an application and the identity and location of each particular person who transmitted such items. SSA should record that it actually received the communication or transmission, who received it, and the date and time received. SSA should also confirm with the applicant that it received an application. *See Legal Considerations in Designing and Implementing Electronic Processes: A Guide for Federal Agencies* at sec. III.C.2.c.

Example 4: Another applicant provides false statements in a telephone interview for SSI benefits. Specifically, he lies about his income and resources, which favorably affects his

eligibility status. He attests to the truth of the false information he provides and agrees to contact SSA to report any inaccuracies or changes once he receives his summary sheet in the mail. The applicant is awarded benefits. After several years, SSA discovers the false statements and the Department decides to prosecute the applicant under 42 U.S.C. § 1383a, for making a false statement to SSA. The applicant then claims that he gave the SSA interviewer accurate financial information and that the interviewer entered his information incorrectly. He also denies having attested to the accuracy of the information under penalties of perjury and instead states that he told the interviewer that he was not sure of the information he provided because he did not have all of his records with him. Further, he claims he never received a summary sheet and thus had no opportunity to discover the "mistake."

- In order to prove that applicants actually receive the application summary sheets that give them the opportunity to review and correct the information entered by the SSA interviewer, a key question will be whether it is sufficient for the government to show that, in the regular course of business, SSA reliably mails summary sheets.
- The Department guidance on electronic conversions recommends that electronic processes include proof that the individual has certified to the truth and accuracy of the information submitted on the application, and has submitted the information under penalty of perjury. *See Legal Considerations in Designing and Implementing Electronic Processes: A Guide for Federal Agencies* at sec. III.C.2.c. SSA has incorporated this into its alternative signature process, but it will be important for SSA to have individuals certify to this as they provide updated information to SSA. *Id.* Also, to help prove the consistency of attestations, it may be important for SSA to unequivocally state in its procedures that no applications will be processed unless an applicant has clearly agreed to the SSA interviewer's attestations.

As the above examples illustrate, electronic processes, in certain respects, may be more complex for fact-finders than paper methods. Therefore, SSA will need to comprehensively detail the new steps to assure AUSAs of the reliability of the process before the AUSAs can convince judges or juries that SSA generated and maintained records of electronic transactions using a trustworthy process. SSA and the Department will need to continue to consult each other in order to understand how any litigation challenges will be resolved. Federal law enforcement agents who work for the SSA's Office of the Inspector General (OIG) will also need to fully understand the new procedures so that they can collect the appropriate evidence during their investigations of Social Security fraud.

IV. Conclusion

As SSA works to enhance its services and stewardship to the public by developing and implementing electronic services, it must exercise its discretion when addressing the new issues that arise relating to this conversion. Of particular importance will be how to protect the government's interests in Social Security fraud-related litigation with the new signature alternatives on applications. To do this, the Department needs available, reliable, and persuasive agency records that are complete, uniform, easily understood, and easily accessible. *See Legal Considerations in Designing and Implementing Electronic Processes: A Guide for Federal Agencies* at sec. I.C.

SSA's new alternative signatures on applications replace the long-standing process that centered on a wet signature on a paper application. For the AUSA, this means a fundamental evidentiary change to Social Security litigation that has traditionally relied on the well-settled rules that have addressed the issues of validity, authenticity, and reliability of paper documents. The new signature alternatives will necessitate some changes in how an AUSA presents electronic evidence.

At this point, no one can provide unequivocal guidelines instructing what program safeguards involving SSA's signature alternatives will ultimately be necessary to protect SSA's legal interests. SSA has presented its new processes to the Department and recognizes that instructional guidance will be ongoing to the Department and to its other stakeholders. It will be important for AUSAs to communicate with the program fraud

investigators from the SSA's OIG, and other SSA employees, to express any issues that may arise concerning the reliability of electronic evidence. By working together to address any litigation issues and to gain a better understanding of the processes, SSA and the Department will be best able to minimize any legal risks and ensure the success of the new alternative signatures.❖

ABOUT THE AUTHOR

❑**Joseph Grow** started with the SSA as a Presidential Management Intern in 1998. He currently works as a Staff Attorney with the SSA's Office of the Inspector General, which, as one of its statutory responsibilities, recommends policies for the purpose of preventing and detecting fraud and abuse in SSA's programs and operations. His government career has also included service with the Federal Deposit Insurance Corporation, the Department of Education, and the Department of State.✠

Prosecuting Employers for Wage and Earnings Violations under the Social Security Act and the Internal Revenue Code

John K. Webb
Special Assistant United States Attorney
Central District of California

I. Introduction

Each year employers file more than 200 million W-2 forms (Annual Statement of Wages and Taxes) with the Social Security Administration (SSA), reporting the wages they have paid to their employees. The Form W-2 shows wages paid the previous tax year for each employee. In addition, employers file quarterly wage reports with the Internal Revenue Service (IRS) on Form 941 (Employer's Quarterly Federal Tax Return), which shows the aggregate amounts of wages the employer paid to all employees during the quarter, and the amounts withheld for income and Social Security taxes under the Federal Insurance Contributions Act (FICA). *See* I.R.C. §§ 3101(a) - 3111(a). Specifically, SSA uses the Form W-2 to credit workers' earnings to their Social Security accounts, which are later used as a basis to calculate Social Security program benefits. The IRS uses Form 941 to ensure the prompt and correct deposit of employment taxes (income and Social Security taxes withheld from employees and the employers' share of the Social Security tax) to the United States Treasury. These wage and earnings reports are critical to the operations of each agency.

- Form W-2 Reports. SSA provides its W-2 information to the IRS, which uses it to ensure that individuals accurately report their income on their tax returns and employers report and pay the appropriate amount of income and Social Security taxes. *See* I.R.C. § 6051(a).
- Form 941 Reports. The IRS provides SSA with Form 941 information, which SSA uses to insure that it has received W-2s from all employers who reported that they withheld

> Social Security taxes and that the aggregate amount of Social Security wages reported on the W-2 forms are equal to the aggregate amount of Social Security wages reported on the 941 forms for each employer. *See* I.R.C. § 6011.

II. Legislative history and statutory authority regarding wages and earnings

Both SSA and the IRS are empowered by Congress to impose strict wage and earnings reporting obligations on employers.

> The Secretary of the Treasury shall make available information returns filed pursuant to part III of subchapter A of chapter 61 of subtitle F of the Internal Revenue Code of 1986, to the Commissioner of Social Security.... The Commissioner of Social Security shall process any withholding tax statements or other documents made available to the Commissioner by the Secretary of the Treasury....

See Pub. L. No. 94-202, § 232, 89 Stat. 1135 (1976) (codified at 42 U.S.C. § 432).

The Commissioner of Social Security is responsible for establishing and maintaining a record of the earnings of all persons who work for employers or who are self-employed and are covered under the various Title II Social Security programs, which include retirement, disability, and survivorship (children and spouse). Specifically, Title II of the Act states:

> On the basis of information obtained by or submitted to the Commissioner of Social Security, and after such verification thereof as the Commissioner deems necessary, the Commissioner of Social Security shall establish and maintain records of the amounts of wages paid to, and the amounts of self-employment income derived by, each individual....

See Section 205(c)(2)(A) of the Social Security Act (the Act); *see also* 20 C.F.R. § 404.801.

The earnings records maintained by SSA and IRS are used to determine entitlement to, and the amount of, benefits that may be payable to a person under the Social Security Title II programs. Eligibility and amount of benefit paid by Social Security is based on a person's earnings as defined in the Act. *See* 42 U.S.C. §§ 401-434; 42 U.S.C. §§ 301-1399; *see also* 20 C.F.R. § 404.801. In addition, Congress requires that SSA certify the earnings records of employees based on the reporting of employers and self-employed individuals.

> There is hereby appropriated to the Federal Old-Age and Survivors Insurance Trust Fund...100 per centum of the taxes imposed by... Chapter 21 of the Internal Revenue Code...with respect to wages... which wages shall be certified by the Commissioner of Social Security on the basis of the records of wages established and maintained by such Commissioner....

See Section 201(a) of the Act.

The Internal Revenue Code (IRC) contains the authority for insuring that the employer collect tax from the wages of employees, and requires that employers and employees keep accurate wage and earnings records. "Every person liable for any tax imposed by this title, or for the collection thereof, shall keep such records... as the Secretary may from time to time prescribe." I.R.C. § 6001 (1994).

Similarly, the IRC requires that employers provide each employee with a W-2.

> Every person required to deduct and withhold from an employee a tax under section 3101 or 3402...shall furnish to each such employee...on or before January 31 of the succeeding year, or, if his employment is terminated before the close of such calendar year, within 30 days after the date of receipt of a written request from the employee if such 30-day period ends before January 31, a written statement showing...(6) the total amount deducted and withheld as tax under section 3101....

I.R.C. § 6051(a).

IRC regulations also require that employers who file 250 or more W-2 wage reports per year must file them on magnetic media, unless the IRS specifically grants the employer a waiver.

> (b)...If the use of Form W-2, W-2P...is required...the information required by such form shall...be submitted on magnetic media....
>
> (c) Exceptions—....(B) In the case of a calendar year or annual period beginning on

or after January 1, 1987—...(2) The person was not required to file 250 or more returns on such form for the preceding year....

(f) Failure to File. If a person fails to file a return on magnetic media when required to do so... such person is deemed to have failed to file the return.

26 C.F.R. § 301.6011-2

III. Importance of the Federal Insurance Contributions Act (FICA)

Employers are required by the IRS to withhold FICA taxes for reporting to SSA. "The tax imposed by section (FICA) 3101 shall be collected by the employer of the taxpayer, by deducting the amount of the tax from the wages as and when paid." *See* I.R.C. § 3102(a).

A. Legislative history of FICA

Congress originated the present income tax withholding system in section 1972 of the Revenue Act of 1942, 56 Stat. 884, charging IRS with responsibility for collection and enforcement of taxes. In 1943 Congress passed the Current Tax Payment Act of 1943, 57 Stat. 126, which also kept tax collection and enforcement responsibilities with the IRS. The current version of FICA was initially passed by Congress in 1954, and it also charged IRS with collection and enforcement responsibilities. Prior to January 1978 employers filed their tax reports and wage reports with the IRS on a quarterly basis. The quarterly FICA tax report forms used were Forms 941 (regular), 942 (household work), and 943 (agricultural work). Attached to these were Schedule A forms showing the detailed amounts of wages for each employee by Social Security Number (SSN). Schedule A forms were first used by SSA to post wages quarterly to each worker's earnings record. In 1976 the wage and earnings reporting system was streamlined and the Combined Annual Wage Reporting (CAWR) system was created to require yearly W-2s to be filed by all employers for each employee, and to report quarterly aggregate employee wage amounts to the IRS on Forms 941. *See* Pub. L. No. 94-202, § 232, 89 Stat. 1135 (1976) (codified at 42 U.S.C. § 432).

B. Memorandum of Understanding (MOU) between SSA and IRS on the CAWR process

Under the authority provided by § 232 of the Act, the IRS and SSA entered into an interagency agreement, a Memorandum of Understanding (MOU), that specified how the CAWR process was to work. Specifically, under the CAWR process, employers continue to file Forms 941, 942, and 943 quarterly with IRS, but no Schedule A forms are filed. Instead, W-2 forms are filed by the employer as the annual wage report for his employees. These reports, in the form of Copy A of the W-2's and a copy of the employer transmittal Form W-3 (or in the form of electronic records of W-2 and W-3 data plus transmittal Form 6559), are filed with SSA annually, on or before the last day of February in the year following the wage reporting year. Included in this process are FICA and non-FICA wage reports and reports from payers of periodic pensions, annuities, retired pay, or Individual Retirement Accounts (IRA's). *See* Programs Operation Manual (POMS) RM 01101.009 (IRS/SA CAWR Agreement).

C. Importance of the MOU

The MOU that exists between the SSA and the IRS is designed to ensure that wage and hour reporting standards are carefully administered, and that employers judiciously adhere to their reporting obligations. The MOU requires that the SSA and the IRS work together to insure the effective and efficient processing of employer wage and earnings reports and to reconcile any discrepancy in reporting by employers. *See* 42 U.S.C. § 432; 20 C.F.R. § 422.114(a). To accomplish the goals of the MOU, employers are instructed by the IRS to file annual wage reports with the SSA on paper Forms W-2 (Wage and Tax Statement) and W-3 (Transmittal of Income and Tax Statements), or by using the equivalent W-2 and W-3 magnetic media reports. *See* 20 C.F.R. § 422.114(a). SSA processes all wage reporting forms for updating to its earnings records and the IRS tax records identifies employer reporting errors and untimely filed forms for IRS penalty assessment action, and takes action to correct any reporting errors identified. *See* 20 C.F.R. § 422.114(a). SSA also processes Forms W-3c (Transmittal of Corrected Income Tax Statements) and W-2c (Statement of

Corrected Income and Tax Amounts), as well as their magnetic media equivalents, that employers are required to file with the SSA when certain previous reporting errors are discovered. *See* 20 C.F.R. § 422.114(a).

D. Employer payment of Employee FICA or State Unemployment Tax

Generally, payment by an employer of the employee's portion of FICA tax, or any payment required to be made by an employee for state unemployment compensation, without deducting it from the employee's wages, is added to the employee's wages. *See* I.R.C. § 3121(a)(6)(A)-(B) *available at* http://www4.law.cornell.edu/uscode/26/3121.html; *see also* Rev Rul 86-14, 1986-1 CB 304 *available at* http://www.taxlinks.com/rulings/1986/revrul86-14.htm. However, if payment is made to an employee for domestic service in a private home of the employer, or for agricultural labor, the amount of the payment is not wages for FICA purposes. *See* I.R.C. § 3121(a)(6) *available at* http://www4.law.cornell.edu/uscode/26/3121.html. In addition, cash payment is not considered FICA wages if it is less than $1,000 in any calendar year for domestic services in the employer's private home, or less than $100 in a calendar year for service not in the course of the employer's trade or business. *See* I.R.C. § 3121(a)(7)(B)-(C) *available at* http://www4.law.cornell.edu/uscode/26/3121.html.

E. What constitutes wages for FICA withholding

Generally, wages for FICA purposes means all remuneration for employment, including the "cash value of all remuneration, including benefits, paid in any medium other than cash." *See* I.R.C. § 3121(a) *available at* http://www4.law.cornell.edu/uscode/26/3121.html. Thus, salaries, fees, bonuses, and commissions on sales or on insurance premiums, are wages if paid as compensation for employment. *See* Reg § 31.3121(a)-1(c). *Id.* The basis upon which remuneration is paid is generally immaterial in determining whether the remuneration constitutes wages, and it may be paid hourly, daily, weekly, monthly, or annually. *See* Reg § 31.3121(a)-1(d) *available at* http://www.irs.gov/irb/2004-10_IRB/ar12.html. How the remuneration is paid is immaterial, and it may be paid in cash or in goods, lodging or clothing. *See* Reg § 31.3121(a)-1(e) *available at* http://www.irs.gov/irb/2004-10_IRB/ar12.html. Pay for employment constitutes wages even if the remuneration is received after termination of the employment relationship between employer and employee. *See* Reg § 31.3121(a)-1(i) *available at* http://www.irs.gov/irb/2004-10_IRB/ar12.html.

F. Reconciliation of SSA and IRS records

SSA provides its W-2 information to IRS, which uses it to ensure that individuals accurately report their income on their tax returns and employers report and pay the appropriate amount of income and Social Security taxes. Likewise, the IRS provides SSA with Form 941 information, which SSA uses to insure that it has received W-2s from all employers who reported that they withheld Social Security taxes and the aggregate amount of Social Security wages reported on the W-2 forms are equal to the aggregate amount of Social Security wages reported on the 941 forms for each employer. *See* POMS RM 01101.002-009 *available at* http://policy.ssa.gov/poms.nsf/poms. (Annual Wage Reporting Process).

IV. Employers' obligation to accurately maintain and report wages and earnings to SSA and IRS

Employers or individuals who knowingly or intentionally furnish false information in connection with earnings records are subject to criminal penalties dealing with fraudulent statements under the Social Security Act (Title II), the Internal Revenue Code (Title 26), and provisions of the federal criminal code (Title 18). *See* 20 C.F.R. § 422.108; 26 C.F.R. §§ 7202 and 7204; and 18 U.S.C. § 1001; *see also* POMS, RM 01101.001 *available at* http://policy.ssa.gov/poms.nsf/poms. The felony fraud provisions of the SSA Title II programs, including fraud in wage and earnings reporting, are found in 42 U.S.C. § 408(a)(1)-(8). Under the Social Security Act, a person defined as an employer or an individual will be guilty of a felony and, upon conviction, will be fined or imprisoned for not more than five years, or both, if the person

> willfully, knowingly, and with the intent to deceive [SSA] as to his true identity (or the true identity of any other person) furnishes or causes to be furnished false information [to SSA] with respect to any information required

> by [SSA] in connection with the establishment and maintenance of records.

42 U.S.C. § 408(a)(6).

Similarly, any employer or individual who makes or causes to be made any false statement or representation

> for the purpose of causing an increase in any payment [by SSA], or for causing any payment to be made where no payment is authorized...as to whether wages were paid or received for employment, or the amount of wages or the period during which wages were paid or the person to whom the wages were paid...shall be guilty of a felony and upon conviction thereof- shall be fined or imprisoned for not more than five years, or both.

42 U.S.C. § 408(a)(1)(A).

In addition, any employer or employee who uses a Social Security Number other than his or her own in the reporting of wage and earnings, or for any purpose, will "be guilty of a felony and, upon conviction thereof shall be fined under Title 18 or imprisoned for not more than five years, or both." 42 U.S.C § 408(a)(7).

A. Importance of accurate wage and earnings reporting to SSA and IRS

Accurate earnings information is essential to SSA. The Title II programs, including those that pay benefits towards retirement, disability, and survivor's benefits for spouses and children, are based on the lifetime earnings of each worker. Thus, the lifetime accumulation of earnings of each worker are used to establish the worker's eligibility for, and the amount of, Social Security benefits they (or their children or spouses) will receive.

B. Social Security benefits based on earnings credits

The amount of Social Security benefits and tax money that the Social Security trust funds are entitled to is based on the earnings recorded in the Social Security accounts of individual wage earners. If SSA fails to record all or part of an individual's annual earnings, the Social Security benefits calculated by SSA for each individual might be counted as less than properly due. In addition, the SSA trust funds would not be entitled to all the tax revenue due them by a fair accounting. Earnings in Social Security-covered employment enable an individual to build sufficient credits, called quarters of coverage, to gain eligibility for Social Security benefits. Once sufficient quarters of coverage are earned and retirement, survivors, or disability conditions are met, SSA uses the amount of earnings to calculate an individual's benefit. *See* POMS RM 01103.009 (Employer's Responsibility for Maintaining Employment Records) *available at* http://policy.ssa.gov/poms.nsf/poms.

C. The self-financing principle of the Title II Social Security programs

The Title II Social Security programs (Retirement, Survivors, and Disability Insurance) were established by Congress to be self-financing, and benefits from the various programs are paid from trust funds that principally receive money generated by dedicated employment taxes (FICA) on designated wages and self-employment income. The Title II programs are in stark contrast to the Title XVI Supplemental Security Income (SSI) program, which is funded from the general tax revenues and is not based on FICA earnings. The self-financing principle has been fundamental to the insurance concept of the Retirement, Survivors, and Disability Insurance programs. The first programs were established in 1935, 1939, and 1966, respectively. *See* 42 U.S.C. § 409(a).

D. Funding methods for the Title II Social Security programs

Three approaches have been used to fund the Title II Social Security programs. The authorizing legislation of the original 1935 Act established an Old Age Reserve Account to maintain a sufficient reserve for payment of benefits under the program. *See* General Accounting Office, GAO/HRD 92-81 Social Security IRS/SSA Reconciliation Efforts *available at* http://gao.gov. By law, the reserve account was structured to receive an annual appropriation, beginning in fiscal year 1937, sufficient to pay benefits and to build up a required reserve. At the same time, also beginning in 1937, the original Act established payroll taxes to be levied on employees and employers based on a percentage of each worker's annual wages. However, because of constitutional concerns, the original Act did not link the

appropriations made to the Old Age Reserve Account with the taxes. Ambiguity about the intention of the original funding was resolved by the Social Security Amendments of 1939, which created a social security trust fund that received revenues on a collection basis. The 1939 Amendments required that the Department of the Treasury (Treasury) transfer to the Social Security trust funds all of the Social Security tax revenue (including interest, penalties, and additions to the taxes) that it collected.

This collection-based funding approach remained in place until 1960, when Congress again changed the funding approach with the enactment of Section 201(a) of the Social Security Act, which simplified the tax collection procedures for both the taxpayer and the government. *Id.* Under Section 201(a), the Social Security trust funds receive revenues based on the total amount of Social Security covered wages certified as being recorded for each individual in SSA's records. Treasury then applies the appropriate tax rate to the certified aggregate amount of Social Security wages recorded by SSA, and transfers revenues directly to the trust funds. Under this funding approach, the trust funds do not receive any interest and penalty revenue derived from the late payment of Social Security taxes. In addition, Section 201(a) provides that the trust funds receive tax revenue for all Social Security wages regardless of whether Treasury collects the taxes. At the beginning of each month, Treasury advances tax revenues to the Social Security trust funds based on estimates of Social Security taxes to be collected during the month. The certification process is periodically adjusted when SSA advises Treasury of the total Social Security wages that SSA has recorded. If the estimates are too high, funds are to be returned to the general revenues of Treasury. *See* POMS RM 02201.001 (Overview of Earnings Adjustment Process) *available at* http://policy.ssa.gov/poms.nsf/poms.

V. Charging decisions and elements of the crime for wage and earnings violations under the Social Security Act–42 U.S.C. §§ 408(a)(1)(A)-(C); 408(a)(6); and 408(a)(7)(B)

Title II of the Social Security Act, cited as 42 U.S.C. § 408(a)(1)-(8), contains the Act's primary criminal provisions and carefully spells out the Act's restraints on fraud involving the reporting of wage and earnings by employers and individuals. Initially enacted as a misdemeanor statute, Congress amended Title II of the Act in 1981 to make Social Security fraud (including SSN misuse) a felony, punishable by five years in prison and a fine up to $250,000. (*See* 1981 Amendments, Pub. L. No. 97-123, 95 Stat. 1659, 1663-64). The following is an analysis of each of the subsections of 42 U.S.C. §§ 408(a)(1)(A), (B), (C); 408(a)(6); and 408(a)(7)(B), including a breakdown of the elements necessary to prove a charge under each, and a brief suggestion of when and how each subsection should be charged.

A. 42 U.S.C. § 408(a)(1)(A)

The elements required to prove a violation of 42 U.S.C. § 408(a)(1)(A) are:

- defendant made a false statement or representation;
- as to whether wages were paid or received for employment; or
- as to the amount of wages or the period during which wages were paid or the person to whom wages were paid;
- used to cause payment or an increase in payment of benefits where no payment is authorized.

See 42 U.S.C. § 408(a)(1)(A).

B. 42 U.S.C. § 408(a)(1)(B)

The elements required to prove a violation of 42 U.S.C. § 408(a)(1)(B) are:

- defendant made a false statement or representation;
- as to whether net earnings from self-employment were derived; or

- as to the amount of such net earnings or the period during which or the person by whom derived;
- used to cause payment or an increase in payment of benefits where no payment is authorized.

See 42 U.S.C. § 408(a)(1)(B).

C. 42 U.S.C. § 408(a)(1)(C)

The elements required to prove a violation 42 U.S.C. § 408(a)(1)(C) are:

- defendant made a false statement or representation;
- as to whether a person entitled to benefits;
- had earnings in or for a particular period, or
- as to the amount of earnings for a particular period;
- used to cause payment or an increase in payment of benefits where no payment is authorized.

See 42 U.S.C. § 408(a)(1)(C).

D. When to charge

While most fraud in Social Security benefits programs involves the falsification of a document or record offered as proof of disability, or occurs when an applicant misrepresents material facts on an application for benefits, a significant amount of fraud involves the false reporting of wages and earnings by employers and employees. Title II of the Act (42 U.S.C. § 408(a)(1)(A)-(C)) makes it a felony to make, for the purpose of receiving any benefit, or increasing any benefit to which the intended recipient is not entitled, a false statement or representation regarding: (1) whether wages were paid or received for employment, the amount of wages, the period during which wages were paid, or the person to whom wages were paid (§ 408(a)(1)(A)); (2) whether net earnings from self-employment were derived, the amount of such earnings, the period during which self-employment earnings were derived, or the person by whom such earnings were derived (§ 408(a)(1)(B)); or (3) whether a recipient of benefits had earnings that might warrant deductions from benefits or the amount of such earnings (§ 408(a)(1)(C)). It is also a felony to cause any such false statement or representation to be made (§ 408(a)(1)). The following are examples of violations that could result in criminal prosecution for false reporting of wage and earnings:

- furnishing false information of identity in connection with the establishment and maintenance of Social Security records, or with the intent to gain information as to the date of birth, employment, wages, or benefits of any person;
- forging or falsifying SSA documents;
- using a Social Security Number obtained on the basis of false information or falsely using the Social Security Number of another person, for the purpose of obtaining or increasing a payment under Social Security or any other federally funded program, or for any other purpose;
- disclosing, using, or compelling the disclosure of the Social Security Number of any person for unauthorized purposes;

Making or causing to be made any false statement or representation as to:

- whether wages were paid or received, the amount of such wages, the period during which wages were paid or received, or the person to whom such wages were paid; or
- whether net earnings from self-employment were received, the amount of such earnings, the period during which such earnings were received, or the person who received them.

See 42 U.S.C. §§ 408(a)(1)(A), (B), (C).

E. Examples of wage and earnings fraud (42 U.S.C. § 408(a)(1))

In *United States v. Mauro*, 80 F.3d 73, 75 (2d Cir. 1996), the Second Circuit affirmed the conviction of a defendant under section (a)(1)(A) because the defendant made false statements to the Social Security Administration. Mauro convinced a man named Bolognese to place Mauro's son on the payroll of Bolognese's company, Atlas. Bolognese issued Mauro's son a payroll check in the amount of $340, withholding $160 in federal and state taxes. Mauro then repaid Bolognese $500. *Id.* Bolognese noted Mauro's son as a "no-show" employee, and the scheme allowed Mauro's son to receive health insurance.

In *United States v. Kaczowski*, 882 F.Supp. 304 (W.D.N.Y. 1994), defendants were convicted of violating section (a)(1)(A) as to "whether wages were paid or received." The defendants created a scheme wherein Kaczowski was placed in a "no-show" job on the payroll of a company called "Kampus Kitchen." *Id*. at 305. The scheme was devised to show that Kaczowski had a legitimate source of income from a company, rather than from illegal gambling proceeds. The defendant argued that no crime had been committed because his codefendant, Gawel, paid federal and state withholding, unemployment insurance, and Social Security taxes. The district court responded that, regardless of the obligation to pay Social Security taxes, defendants had made a false statement regarding the source of the income, which goes to whether "wages were paid or received."

In *United States v. Krogstad*, 576 F.2d 22, 23 (3d Cir. 1978), the Third Circuit affirmed the conviction of a defendant who filed false employer tax returns by understating the true number of its employees, and failing to pay the appropriate amount of income and Social Security taxes withheld as to such employees.

F. 42 U.S.C. § 408(a)(6)

The elements required to prove a violation of 42 U.S.C. 408(a)(6) are:

- defendant willfully, knowingly, and with intent to deceive as to his true identity or the identity of another person;
- furnishes, or causes to be furnished, false information to SSA;
- with respect to any information used by SSA to establish or maintain records.

See 42 U.S.C. § 408(a)(6).

A person may also be subject to criminal penalties under § 408(a)(6) for furnishing false information in connection with earnings records. *See also* 20 C.F.R. § 422.108. For example, criminal liability arises under 42 U.S.C. § 408(a)(6) when an employer,

> knowingly, and with intent to deceive the Commissioner of Social Security as to his identity furnishes, or causes to be furnished false information to the Commissioner...with respect to any information required...in connection with the establishment and maintenance of the records.

This usually occurs when an employer, who knows that an employee is working while using a false Social Security Number and/or identity, makes false statements in wage and earnings reports to SSA (Form W-2) and to the IRS (Forms W-2, 940, 941) as to such wages and earnings or identity. This charge is especially applicable to companies who frequently hire individuals that the company suspects may have provided false identity documents in order to work. Prosecution of vulnerable employees for trying to make a living in order to survive is unappealing to prosecutors for a number of reasons. However, prosecution of corporate offenders whose lax hiring policies are the source of false wage and earnings reporting is a more practical and effective approach to prosecuting wage and earnings cases. In addition to SSA felony charges, an employer can face Title 18 felony charges for making false statements on IRS documents W-2, W-3, and 940 (18 U.S.C. § 1001), as well as immigration fraud (18 U.S.C. § 1546) for false I-9 and W-4 Forms.

G. 42 U.S.C. § 408(a)(7)(B)

The elements required to prove a violation of 42 U.S.C. § 408(a)(7)(B) are:

- false representation of a Social Security account number;
- with intent to deceive;
- for any purpose.

See United States v. Means, 133 F.3d 444, 447 (6th Cir. 1998) (setting forth the elements for prosecution of a case under 42 U.S.C. § 408(a)(7)(B)). *See also United States v. McCormick*, 72 F.3d 1404, 1406 (9th Cir. 1995).

The felony provisions of 42 U.S.C. § 408(a)(7)(B), which deal with the misuse of a Social Security Number, are particularly effective in charging cases involving wages and earnings fraud when an individual or company has attempted to circumvent wage and earnings laws by using false Social Security Numbers to hire employees who might otherwise be ineligible to work. In recent years, it has become common for service companies to knowingly hire individuals using false identity documents. Some rogue employers have gone so far as to provide Social

Security Numbers for individuals known by the employer to be illegal and to help the individuals complete wage and earnings reporting documents (W-4, W-2, and 940 forms). Each of the reporting forms that SSA and IRS require an employer to complete must include a Social Security Number. Thus, each time a false number is reported by an employer or employee on a wage and earnings document required by an employer, it constitutes a felony violation of § 408(a)(7)(B). The charging standard, "for any purpose," is broad and self-explanatory, and any false representation of a Social Security Number, with an intent to deceive, is actionable conduct that may be charged as a felony under § 408(a)(7)(B). *See United States v. Silva-Chavez*, 888 F.2d 1481 (5th Cir. 1989); *United States v. Perez-Campos*, 329 F.3d 1214 (10th Cir. 2003); *United States v. Ettienne*, No. 02-4850, 2003 WL 21313165 (4th Cir. Jun. 6, 2003); *United States v. Charles*, 949 F.Supp. 365 (D.V.I. 1996).

In the case of *United States v. Chapman*, No. 98-5093, 1999 WL 551919 (6th Cir. July 21, 1999), the Sixth Circuit convicted the defendant, her supervisor, and a few others for Social Security fraud in violation of 42 U.S.C. § 408(a)(7)(B). The individuals engaged in an illegal scheme to obtain applications by locating homeless persons and having them sign up for TennCare. *Id*. at *2. The defendant was a part-time marketing representative for Omnicare, a managed care organization contracting with TennCare, a program administered by the state of Tennessee that provided medical benefits to Medicaid-eligible and to uninsured/uninsurable persons. The defendant provided application forms to subcontractors who would then fill in information on the forms by using names from telephone directories and fabricating Social Security Numbers and dates of birth. *Id*. at *3.

VI. Charging decisions and elements of the crime for wage and earnings violations under the Internal Revenue Code—I.R.C. §§ 7202, 7204, 7205, & 7206

I.R.C. § 7202 criminalizes both the willful failure to collect taxes and the willful failure to account truthfully for and pay over taxes. A conviction for violating § 7202 can result in fines of up to $10,000, imprisonment for up to five years, or both. I.R.C. § 7204 provides the exclusive sanction for an employer who furnishes employees with a false W-2 statement. I.R.C. § 7206 makes it a felony for any employer to willfully fail to "collect, truthfully account for, and pay over" any tax that the employer has a duty to collect. What follows is a description of I.R.C. §§ 7202, 7204, and 7206, including a breakdown of the elements necessary to prove a charge under each, and a brief suggestion of when and how each subsection should be charged.

A. I.R.C. § 7202

The elements required to prove a violation of I.R.C. § 7202, Part 1: Failure to Collect Tax are:

- defendant had a legal duty to collect, account for, and pay over a tax;
- defendant failed to collect that tax; and
- defendant acted willfully.

See I.R.C. § 7202.

Prosecutions for willful failure to collect a tax are usually charged when there is a failure by an employer to properly withhold the statutorily-required amounts from employees' wages, and when the employer is negligent in paying over such amounts to the government.

The elements required to prove a violation of I.R.C. § 7202, Part 2: Failure to Truthfully Account for Tax are:

- defendant had a legal duty to collect, account for, and pay over tax;
- defendant failed to truthfully account for and pay over that tax; and
- defendant acted willfully.

See I.R.C. § 7202.

Prosecutions for "willful failure to truthfully account for and to pay over a tax" are usually charged when an employer withholds taxes from employees' paychecks but fails to account for or pay over the withheld amount to the government at the end of the quarter. *Id.*

B. I.R.C. § 7204 (misdemeanor)

If an employer willfully fails to furnish a Form W-2 to an employee as required by 26 C.F.R. §§ 6051 and 6053(b), or if an employer

furnishes a false or fraudulent Form W-2 to an employee, the employer will be subject to a penalty of $50 for each violation. *See* 26 C.F.R. § 6674. Any penalty assessed under I.R.C. § 7204 is collected in the same manner as the Social Security FICA taxes payable by employers under 26 C.F.R. § 3111. The $50 civil penalty may be imposed in addition to any criminal penalty charged against an employer under I.R.C. § 7204. Providing false W-2's to employees can be sufficient to prove an aiding and assisting offense pursuant to § 7204. *See United States v. Gambone*, 180 F. Supp. 2d 660 (E.D.Pa. 2001).

C. I.R.C. § 7205 (misdemeanor)

Section 7205 is usually charged in response to tax avoidance schemes. For example, whenever an individual/employee willfully executes a false W-4 or W-9 in connection with wages and earnings withholding for reporting purposes, or files a return that he believes may contain material factual misrepresentations, he may be charged with a misdemeanor violation of I.R.C. § 7205.

As an example, employees of a company involved in a strike and lock-out were encouraged to work using false names and Social Security Numbers in order to by-pass features of the company's payroll and personnel system that identified and rejected locked-out employees. Some employees who worked during the lock-out filed false W-4 and I-9 forms using Social Security Numbers and names that were totally fictitious or borrowed from their spouses, children, or other relatives. The bogus W-4 and I-9 forms were filed with their employer (and coconspirator), resulting in the reporting of false wage and earnings (W-2 and Form 941) to the IRS and SSA.

D. I.R.C. § 7206 (felony)

The elements required to prove a violation of I.R.C. § 7206, Willful False Statement are:

- defendant signed a federal income tax document containing a written declaration that it was being signed under the penalties of perjury;
- defendant knew that the document contained false information; and
- defendant willfully and intentionally made the false statement.

The elements required to prove a violation of I.R.C. §7206, Fraudulent Aid or Assistance are:

- defendant assisted, procured, counseled, advised, or caused the preparation and presentation of a return;
- the return was fraudulent or false as to a material matter; and
- defendant acted willfully.

See United States v. Perez, 565 F.2d 1227, 1234 (2d Cir.1977)

For a conviction under § 7206, proof of willful making or subscribing, or willfully assisting in the preparation of a false return, is required. Section 7206 is also a felony statute, and in order to get a conviction, the government need not prove a tax deficiency.

Whenever an employer or individual willfully makes a false statement on any reporting document (such as a W-2, W-3, or Form 941), which is verified by a written declaration made under penalties of perjury, it is a felony that may be punishable by a fine of not more than $100,000 ($500,000 in the case of a corporation), or up to three years imprisonment, or both, together with the costs of prosecution. *See* I.R.C. § 7206(1). The penalties are the same whenever an employer or individual willfully aids or assists in, or advises in the preparation or prosecution of a return, affidavit, claim, or other document that contains fraudulent or false material statement. *See* I.R.C. § 7206(2).

As an example, owners of a company participated in a scheme designed to reduce the amount of tax paid by the employees and the company, by paying employees partially or completely for their services with a check charged against the company's operating account, with the remainder being charged against the company's wages account. Employee withholding for federal income tax, state income tax, and FICA, was charged only from the checks written from the wages account. No withholding was done for payment of wages charged against the company's operating account, nor was the payment of employee wages from the operating account reported on the W-2 forms provided to the employees and filed with the IRS by the company. Employees who participated in the scheme used

the false W-2 forms to prepare their understated federal income tax returns. Further, the portion of the employee's wages payable from the company's operation account was to a nonexistent person or a relative of the employee, usually a child, who was not employed by the company. Defendants were charged with aiding and assisting in the preparation and filing of a false federal income tax return, in violation of I.R.C. § 7206, and with conspiring to defraud the federal government by aiding and assisting in the preparation of the false returns through understated W-2 forms in violation of 18 U.S.C. § 371. *See United States v. Isaksson*, 744 F.2d 574 (7th Cir. 1984). If an employer is convicted under the criminal provisions of § 7206, the employer will be guilty of a felony and subject to imprisonment. *See* I.R.C. § 7206.

In *United States v. Romanow*, 509 F.2d 26 (1st Cir. 1975), co-owners of a furniture store were convicted of perjury where they filed falsely inflated Employers Quarterly Tax Returns, even though the IRS did not rely on the false information in calculating the tax, because materiality is measured by a statement's potential, rather than its actual, impact.

VII. Conclusion

Accurate earnings information is essential to SSA because the earnings of workers are instrumental to the concept behind SSA benefits programs that are critically important to the lives of many Americans. Failure to properly collect and account for FICA taxes from employee wage and earnings can severely damage the SSA Title II Programs and short change many Americans, including those that pay benefits towards retirement, disability, and survivor's benefits for spouses and children. Aggressive prosecution of employers who violate wage and earnings laws benefits all Americans.❖

ABOUT THE AUTHOR

❑**John K. Webb** is a Senior Attorney with the Office of Chief Counsel for the Inspector General, Social Security Administration, and a Special Assistant United States Attorney with the United States Attorney's office for the Central District of California, Los Angeles, where he serves as Identity Theft Coordinator. He is responsible for prosecuting federal crimes involving identity fraud and abuse of Social Security programs, and has participated in the indictment and prosecution of individuals related to the terror attacks of 9/11, as well as the planning and implementation of Operation Tarmac/Operation Safe Harbor in Phoenix and Los Angeles. Mr. Webb has served as an instructor at the National Advocacy Center and is a frequent lecturer on the topics of Identity Theft, Social Security Number Misuse, and Federal Benefits Fraud. Mr. Webb is a regular contributor to the *United States Attorneys' Bulletin*.✠

Overview of the Social Security Administration's Civil Monetary Penalty Program: Applying Sections 1129 and 1140 of the Social Security Act

Julia Chu
Attorney
Office of Chief Counsel to the Inspector General
Social Security Administration

Jonathan Morse
Program Specialist
Office of Chief Counsel to the Inspector General
Social Security Administration

I. Introduction

The Social Security Administration (SSA) became an independent agency with the passage of the Social Security Independence and Program Improvements Act of 1994 (SSIPIA), Pub. L. No. 103-296, 108 Stat. 1464 (1995). At this time, the duties of the Secretary of Health and Human Services in Social Security cases were transferred to the Commissioner of Social Security (Commissioner), effective March 31, 1995. 42 U.S.C. § 901. In addition, the SSIPIA created an independent Social Security Administration, Office of the Inspector General (SSA-OIG), to which the Commissioner delegated certain civil monetary penalty (CMP) authority on June 28, 1995. *Id.* The CMP authority is a key part of the SSA-OIG's efforts to eradicate fraud, waste, and abuse in Social Security programs.

The CMP program balances the OIG's mission of protecting Social Security programs from fraud with the Social Security Administration's goal of being a service-oriented government agency, by administering reasonable penalties aimed at dissuading individuals or entities from making false statements or representations regarding SSA benefits, programs, or symbols. The CMP process is less formal and less expensive than federal civil court proceedings, and thus is effective in cases with smaller damages where civil and criminal prosecution is often impractical. SSA-OIG reviews more than 100 CMP cases per year, and between April 2002 and March 2004, the OIG imposed $2.4 million in penalties and assessments through civil monetary penalties under sections 1129 and 1140 of the Social Security Act, 42 U.S.C. § 1320a-8, b-10. *See* Social Security Administration, Office of the Inspector General Semiannual Report to Congress (June 2004).

This article details the statutory background of sections 1129 and 1140, including the 2004 amendments to enhance penalties and close loopholes; discusses the process by which CMPs are enforced under sections 1129 and 1140; and draws attention to the way in which the SSA-OIG coordinates with the U.S. Attorneys' offices (USAO) to effectively administer the program.

II. Section 1129 of the Social Security Act—false statements and representations

Section 1129 imposes civil monetary penalties against those who have made, or caused to be made, a false statement and/or representation to SSA, which they knew or should have known was false or misleading.

A. Statutory background

Section 1129 of the Social Security Act, 42 U.S.C. §1320a-8, was enacted in 1935 as part of the Social Security Act, Pub. L. No. 74-271 (1935). Specifically, the provision delegates authority to the Commissioner to impose

monetary penalties and assessments against any individual, organization, agency, or other entity (i) who makes or causes to be made a false or misleading statement or representation of a material fact; (ii) for use in determining initial or continuing rights to Old-Age, Survivors, and Disability Insurance (OASDI) or supplemental security income (SSI) benefit payments; (iii) if the person knew or should have known that such statement was false, misleading, or omits a material fact.

The statute defines a material fact as "one in which the Commissioner of Social Security may consider in evaluating whether an applicant is entitled to [benefits]." 42 U.S.C. § 1320a-8(a)(1). This language provides the OIG latitude in determining what constitutes a material fact. Often, the false statement is made on an SSA benefits application question pertaining to work activity or income. The OIG, however, has successfully used other means, such as a signature on a Social Security benefits check, or an oral false statement to a claims representative, as a false statement of material fact. The penalty for each false statement or representation is up to $5,000. In addition, the Commissioner may impose an assessment in lieu of damages of up to twice the amount of benefits fraudulently received as a result of the false statement or representation. 42 U.S.C. § 1320a-8(a)(1).

In the spring of 2004, Congress passed H. Rep No. 743, Social Security Protection Act of 2004, Pub. L. No. 108-203, 118 Stat. 493 (2004), which amends section 1129 by broadening the scope of the civil monetary penalty program. The amendment adds new categories for penalties against representative payees with respect to wrongful conversions, and individuals who withhold material facts from the Social Security Administration.

The first amendment extends the civil monetary penalty provisions to representative payees (including individuals, organizations, agencies, or other entities) who wrongfully convert a payment intended for a beneficiary. These representative payees are subject to a penalty of up to $5,000 for each such wrongful conversion.

The second amendment under section 1129 allows SSA-OIG to impose civil monetary penalties and assessments for the failure to come forward and notify SSA of changed circumstances that affect eligibility or benefit amounts, when such person knows or should know that the failure to come forward is misleading.

Previously, under section 1129, the OIG was only able to impose a civil monetary penalty and assessment against individuals who made false statements or representations or omitted a material fact on an SSA form or to an SSA employee; thus, this amendment closes a loophole. This amendment, however, is not intended to cover individuals who do not have the capacity to understand that their failure to come forward is misleading.

B. Civil monetary penalty process under section 1129

The OIG Fraud Hotline receives tips on possible benefits fraud and reports the cases to the Office of Investigations (OI). In instances where it appears individuals may have made a false statement to receive benefits, OIG Special Agents will conduct an investigation and prepare Reports of Investigations (ROI) detailing their findings. If fraud or false statements are found, the ROI is submitted to the local USAO for review. The USAO has the option to accept or decline the case. If the case is accepted for civil prosecution, there is no CMP process. If the case is accepted for criminal prosecution, the Office of Chief Counsel to the Inspector General (OCCIG) will work with the U.S. Attorney and, at the conclusion of the criminal case, determine whether the case warrants a civil monetary penalty.

If the USAO declines the case, both civilly and criminally, the OIG Special Agent will forward the ROI to OCCIG for review. The USAO will decline cases for many reasons, though most often because the possible penalty or recovery amount does not warrant the resources of the federal court system. Therefore, the CMP process becomes a cost-effective alternative to a federal court action. Attorneys for OCCIG will screen potential CMP cases using criteria such as whether there is a false statement, whether there is a criminal and civil declination from the USAO, the amount of the overpayment, and the potential resources of the subject.

If the case meets the basic criteria for a possible CMP, OCCIG accepts the case, and an attorney will issue an initial letter to the subject. Section 1129 does not require an initial letter, but

it provides notice to the individual that the Office of Inspector General received information indicating that the person may have knowingly made, or caused to be made, false statements and/or misleading representations to the Social Security Administration. In this letter, the individual is asked to contact the attorney and to submit a financial disclosure form which provides information about sources of income and outstanding debts. In addition to providing notice to the subject, the initial letter serves as an opportunity for the individual to disclose additional relevant facts that could alter OIG's findings, mitigate the penalty, and/or lead to a settlement agreement. The subject has thirty days from the receipt of the initial letter to respond.

If an individual fails to respond to the letter within thirty days, Chief Counsel will issue a demand letter that proposes to impose a penalty against the subject for violation(s) of section 1129. Pursuant to 42 U.S.C. § 1320a-8(c), Chief Counsel will consider the following factors to determine a penalty amount:

- the nature of the statements and representations and the circumstances under which they occurred;
- the degree of the subject's culpability;
- the subject's history of prior offenses in connection with Social Security programs;
- the subject's financial condition; and
- such other matters as justice may require.

42 U.S.C. § 1320a-8(c).

OCCIG also has the authority to double the overpayment when calculating a CMP. 42 U.S.C. § 1320a-8(a)(1). By doubling the assessment in lieu of damages, OCCIG can take advantage of greater collection authority for recovering a penalty and overpayment than if the Agency were to collect the overpayment separately.

The demand letter will also notify the subject of his right to a hearing, which the subject must request from the Departmental Appeals Board of the United States Department of Health and Human Services (DAB), within sixty days of receipt of the demand letter. In accordance with 20 C.F.R. § 498.126, OCCIG may settle with the subject at any time prior to a final determination.

Once OCCIG has sent a demand letter, the sixty-day appeal window continues to toll during the settlement process. Settlements are most successful with subjects currently receiving Social Security benefits, as the penalty and overpayment can be withheld from monthly benefits. Between April 2002 and March 2004, OCCIG settled forty-eight cases at an average penalty and assessment of over $7,000 per case. *See* Social Security Administration, Office of the Inspector General, Semiannual Report to Congress (June 2004). These penalties are in addition to monies collected and applied by the Agency towards the overpayment in such cases.

If the subject does not request a hearing within sixty days, the Chief Counsel will initiate default proceedings, whereby an attorney will send a default letter to notify the subject that the sixty-day appeal window has lapsed and the penalty and/or assessment will be forwarded to SSA's collections department.

In 2002 OIG began an investigation into an individual who allegedly used his wife's name and SSN at his place of employment in order to continue collecting SSI benefits under his own name. An investigation by OIG Special Agents revealed that his employer, a Michigan car dealership, was in fact allowing the individual to collect paychecks under his wife's name, and had been doing so for more than five years. The case was submitted and accepted by the USAO for the Eastern District of Michigan, which entered into a plea agreement with the individual, requiring him to make restitution to SSA in the amount of $91,000. In addition, the OIG sent an initial CMP letter to the dealership, alleging the corporation made intentional false statements on the IRS W-2 and W-4 wage reports for the individual. The letter cited section 1129(a)(1), stating that the Commissioner may impose a penalty against any person (or entity) that has caused to be made a false and/or misleading statement or representation of a material fact for use in determining any initial or continuing right to or amount of benefits or payments under Title XVI of the Social Security Act. 42 U.S.C. § 1320a-8(a)(1) (2004). The OIG argued the wage reports were false statements of material fact because had SSA known of the individual's employment at the dealership, the individual would have been subject to a disability re-determination based on his income from the employment. The dealership entered into a settlement with the OIG for $25,000.

III. Section 1140 of the Social Security Act—Misuse of SSA program words, emblems, and symbols

Section 1140 of the Social Security Act, 42 U.S.C. § 1320b-10, prohibits or restricts various activities involving the use of SSA symbols, emblems, or references, and provides for the imposition of civil monetary penalties with respect to violations of section 1140.

The SSA may enforce section 1140's prohibition on misleading advertisements by imposing civil penalties through its OIG and by seeking injunctive relief. *See* 42 U.S.C. §§ 1320b-10(c); 1320a-7a(k).

A. Statutory background

In 1987 the House Ways and Means Subcommittee on Social Security held a hearing on deceptive mailing practices that were misleading and misinforming Social Security beneficiaries. *See Misleading and Deceptive Mailings to Social Security Beneficiaries: Hearing before the Subcomm. on Social Security*, 99th Cong. (1987).

In response to problems identified at the February 1987 hearing, Congress enacted section 1140 as part of the Medicare Catastrophic Coverage Act of 1988, Pub. L. No. 100-360, 102 Stat 683 (1988). As originally enacted, the provision only prohibited the misuse of SSA and Medicare words, letters, symbols, and emblems in situations where a person "knew or should have known" that use of such terms would convey a false impression of governmental connections with SSA or the Health Care Financing Administration (HCFA). This legislation also authorized the Secretary of Health and Human Services (HHS) to impose penalties not to exceed $5,000 per mass mailing, with a penalty cap of $100,000 per year.

In May 1992 extensive hearings were held regarding the adequacy of section 1140 in preventing misuse of the SSA's and HCFA's distinctive program words, letters, symbols, and emblems. Ultimately, Congress strengthened various enforcement and penalty provisions within section 1140. Among other things, the Social Security Independence and Program Improvements Act of 1994 (Pub. L. No. 103-296): (1) eliminated the annual penalty cap to provide stronger deterrence; (2) redefined a violation to be each individual piece of mail rather than each mass mailing; (3) provided an alternative standard of liability triggered without regard to the actor's knowledge or intent and encompassing how a mailing "reasonably could be interpreted or construed" by consumers; and (4) made disclaimers of affiliation with the Government ineffective as a defense against liability. *See* H.R. Rep. No. 103- 506 at 71-72 (1994), *reprinted in* 1994 U.S.C.C.A.N. 1494, 1524-25.

Today, section 1140(a)(1) of the Social Security Act, 42 U.S.C. § 1320b-10(a)(1), prohibits the

> use, in connection with any item constituting an advertisement, solicitation,...or other communication,...alone or with other words, [or] letters,...the words..."Social Security,"..."Social Security System,"..."Supplemental Security Income Program,"...the letters "SSA,"..."SSI," or any other combination or variation of such words or letters,...in a manner which such person knows or should know would convey, or in a manner which reasonably could be interpreted or construed as conveying, the false impression that such item is approved, endorsed, or authorized by the Social Security Administration...or that such person has some connection with, or authorization from, the Social Security Administration....

A solicitation may violate this section even if it contains disclaimers. Section 1140(a)(3) provides that:

> Any determination of whether the use of one or more words...[or] letters...(or any combination or variation thereof) in connection with [a solicitation]...is a violation of this subsection shall be made without regard to any inclusion in such [solicitation]...of a disclaimer of affiliation with the United States Government or any particular agency or instrumentality thereof. (emphasis added).

Most recently, Congress further extended the enforcement authority under section 1140 with the enactment of H.R. 743, Social Security Protection Act of 2004, Pub. L. No. 108-203, 118 Stat. 493 (2004).

The first amendment to section 1140 provides for the imposition of a penalty against individuals

or groups who offer to assist a person in obtaining products or services for a fee that the SSA otherwise provides free of charge. Congress determined, for example, that business entities have offered assistance to individuals in changing their names (upon marriage) or in obtaining a Social Security Number (upon the birth of a child) for a fee, even though these services are directly available from the SSA for free. S. Rep. No. 108-176, at 16 (2003). The new amendment requires an individual or group who charges a fee for such product or service to provide written notice on the solicitation/mailing stating that the service is available for free from the SSA. The Commissioner has the authority to set the standards for the notice with respect to content, placement, and legibility. The goal of this regulation is to prevent solicitations/mailings which embed such notices among other text, or place the notice in small typeface in an attempt to hide the fact that the services are provided free of charge by the SSA.

The amendment provides exceptions for persons serving as a claimant representative in connection with a claim arising under Title II, Title VIII, or Title XVI, and for persons assisting individuals in a plan with the goal of supporting themselves without Social Security disability benefits.

The second amendment to section 1140 incorporates the additional terms, "Death Benefits Update," "Federal Benefit Information," "Funeral Expenses," or "Final Supplemental Plan," since marketers use these words to give the false impression that their solicitations/mailings are connected to, or authorized by the SSA. Social Security Protection Act of 2004, Pub. L. No. 108-207, 118 Stat. 493 (2004).

B. Civil monetary penalty process under section 1140

OCCIG attorneys screen potential 1140 CMP cases by analyzing whether organizations or persons improperly used program words, letters, symbols, or emblems in a misleading or deceptive manner. If the case meets the criteria for a possible 1140 CMP, OCCIG accepts the case and an attorney will issue an initial letter to the subject. The initial letter requests a voluntary "cease and desist" from committing acts that violate section 1140. While section 1140 does not require an initial letter, it serves to inform the subject that the OIG received information indicating that it has unlawfully used SSA program words, letters, symbols, or emblems in a deceiving manner. In this letter, an OCCIG attorney requests that the target contact OCCIG and provide evidence of their compliance within thirty days of receiving the initial letter. During this period and any time prior to a final determination, OCCIG has the authority to engage in settlement agreements with the target. 20 C.F.R. § 498.126.

Once OCCIG receives the referred complaint, an investigation into the allegations of the complaint begins. During the investigatory stages, OCCIG may request assistance from the USAO to seek and obtain injunctive relief against those in violation of the statute. Such relief may include a court order to:

- stop the violative communications;
- permit an administrative search of business premises;
- freeze assets in anticipation of the imposition of a penalty (to ensure that there will be funds available to pay for any civil penalties that are imposed on defendants, to pay restitution to consumers defrauded by the defendants or to disgorge the profits of their fraud); and/or
- impose a mail stop on the violators' incoming U.S. mail.

42 U.S.C. §§ 1320a-7a(k); 1320b-10.

If a response from the subject is not received within thirty days from receipt of the initial letter, Chief Counsel will issue a demand letter to assess a penalty against the organization or individual. Regulations promulgated by the SSA pursuant to the Act, which are set forth at 20 C.F.R. Part 498, govern the administrative procedures for imposing civil penalties under section 1140. These regulations provide that a party may appeal the SSA-OIG's proposal that civil penalties be imposed under section 1140, to an Administrative Law Judge, the Department of Health and Human Services Departmental Appeals Board, the Commissioner of Social Security, and the appropriate Circuit Court of Appeals, respectively. 20 C.F.R. §§ 498.202; 498.221; 498.222.

Pursuant to 20 C.F.R. § 498.106(b), Chief Counsel will consider the following factors in determining the penalty amount:

- the nature and objective of the advertisement, solicitation, or other communication, and the circumstances under which they were presented;
- the frequency and scope of the violation and whether a specific segment of the population was targeted;
- the prior history of the individual, organization, or entity in their willingness or refusal to comply with informal requests to correct violations;
- the history of prior offenses of the individual, organization, or entity in their misuse of program words, letters, symbols, and emblems;
- the financial condition of the individual or entity; and
- such other matters as justice may require.

If the subject does not request a hearing within sixty days from receipt of the demand letter, Chief Counsel will initiate default proceedings, whereby an attorney will send a default letter to notify the subject that the sixty-day appeal window has lapsed and the penalty and/or assessment will be forwarded to SSA's collections department.

In the case of *United States v. Fed. Record Serv. Corp.*, No. 99 Civ. 3290, 1999 WL 335826 (S.D.N.Y. May 24, 1999), OCCIG worked with the USAO to file a civil action against the defendants for injunctive relief under section 1140 of the Social Security Act, 42 U.S.C. § 1320b-10, and the mail and wire fraud civil injunction statute, 18 U.S.C. § 1345. OCCIG sought to prevent the defendants from continuing to mislead and defraud the public in solicitations for services that purported to assist individuals in obtaining a Social Security Number for a newborn child or changing the name on a social security card after marriage. The USAO helped OCCIG obtain a preliminary injunction against the defendants, which directed the U.S. Postal Service to detain all incoming mail addressed to the Federal Record Service Corporation. The injunction was a great advantage to OCCIG in eventually persuading the defendants to reach a settlement agreement.

IV. Collection authority

SSA has several options for collecting outstanding penalties and assessments. Pursuant to 20 C.F.R. § 498.128, the civil monetary penalty and assessment under sections 1129 and 1140 may be recovered by:

- a civil action in a United States district court;
- reduction in the tax refund to which one is entitled, as permitted under 31 U.S.C. § 3720A;
- decreasing any payment of monthly insurance benefits under Title II or payments under Titles VIII or XVI of the Act;
- authorities provided under the Debt Collection Act of 1982, *as amended*, to the extent applicable to one's debt;
- deduction of the amount one owes from any later amount owed to him by the United States; or
- any combination of the foregoing.

V. Subpoena authority

Pursuant to the Inspector General Act of 1978, *as amended*, 5 U.S.C. app. 3 § 6(a)(4), the SSA-OIG has the authority to issue subpoenas. With regard to 1129 CMP cases, the subpoena power enables OIG to obtain financial information (in accordance with the Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-3422), such as bank records, to calculate overpayments. In specific circumstances, OIG will also subpoena documents on property ownership and assets. Similarly, in 1140 CMP cases, OIG will exercise its subpoena authority to obtain information, such as mailings and bank records, to determine the number of violations.

VI. Conclusion

The CMP program is a valuable tool with which the Social Security Administration protects the Agency's program integrity against fraud, waste, and abuse, as well as the public's trust in the Agency. The Agency relies on the assistance of multiple components, in particular the USAOs, to address violations of sections 1129 and 1140. The Agency hopes to continue collaborative efforts with the USAOs to not only strengthen enforcement authority, but also to help deter future section 1129 and section 1140 violations.❖

ABOUT THE AUTHORS

❑**Julia Chu** is a an attorney with the Office of Chief Counsel to the Inspector General. She joined the Counsel's office in September 2003, and has since worked on the prosecution of civil monetary penalty cases and drafting regulations for expanded civil monetary penalty authority.✠

❑**Jonathan Morse** is a program specialist with the Office of Chief Counsel to the Inspector General. He joined the Counsel's office in the Fall of 2002, and has since worked on the prosecution of civil monetary penalty issues and legislative matters.✠

Request for Subscription Update

In an effort to provide the UNITED STATES ATTORNEYS' BULLETIN to all **federal law enforcement personnel** who wish to receive it, we are requesting that you e-mail Nancy Bowman (nancy.bowman@usdoj.gov) with the following information: Name, title, complete address, telephone number, number of copies desired, and e-mail address. If there is more than one person in your office receiving the BULLETIN, we ask that you have one receiving contact and make distribution within your organization. If you do not have access to e-mail, please call 803-576-7659. Your cooperation is appreciated.